(Online) ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 14, No. 2, April 2026, pp.79-102

Intelligent comprehensive privacy protection system for location-based services

Omar F. Aloufi[1, 2*], Ahmed S. Alfakeeh[1], Fahad M. Alotaibi[1], Samah A. Abbas[3]

[1] Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia

[2] Department of Information Systems, College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia

[3] Department of Management Information Systems, Faculty of Economics and Administration, King Abdulaziz University, Jeddah, Saudi Arabia

* Corresponding author E-mail: oaloufi0017@stu.kau.edu.sa

ABSTRACT

Recently, location-based systems (LBS) have been proven to be an essential element of smart cities due to the valuable benefits they provide to users searching for their nearest Points of Interest (PoI), facilitating daily life activities. However, privacy protection is a major concern in LBS, where attackers can apply advanced attacks, such as location homogeneity, semantic location and query analyzing attacks, to infer sensitive information about the private lives of LBS users. Therefore, protection of location privacy as well as query privacy is necessary to increase the trust of users in LBS. To address this issue, we present the Intelligent Comprehensive Privacy Protection (IntCPP) system as an enhancement of our previous work by employing a deep-learning technique. The Foursquare weekly trajectory dataset is selected to train the proposed system using the long short-term memory (LSTM) technique with an efficient pre-processing stage to adopt time-series data to the environment of LSTM. Evidence of the IntCPP system's superiority is provided through comparison to two intelligent dummy-based systems as well as three traditional dummy-based systems. In terms of accuracy, a (0.05) enhancement degree is achieved, while in terms of entropy, cumulative resistance against attacks, and average cumulative cache hit ratio, (2.0, 100%, 0.17) enhancement degrees are achieved, respectively.

Keywords: LBS, Entropy, Resistance, Attacks, Privacy Protection, LSTM, Pre-Processing

1. Introduction

Advanced technologies such as the Internet of Things (IoT) and cloud computing contribute to providing effective infrastructure to develop advanced systems and applications that enrich smart cities. IoT with smart devices equipped by sensors enables to collect data in real time. The data is stored in cloud to make it available for retrieving anytime and anywhere. The stored data is used to develop systems and applications that enable people to conduct their daily activities easily and quickly [1]. One of the most important systems used in smart cities is recommendation systems. Among recommendation systems, location-based services (LBS) attracts users through offering an easy way to search for the nearest Points of Interest (PoI), such as the nearest medical centers, sport clubs, parks, and Ubers. Employing LBS recommendation systems brings valuable benefits to users, saving them time and effort [2].

Using LBS recommendation systems can be a critical tool to save the life of an affected person, allowing the user to find nearest medical centers as a POI in an emergency situation, such as an accident. Another scenario that highlights the invaluable benefits of LBS recommendation systems is searching for the nearest plumber to repair broken water pipes in homes, which can lead to significant financial losses if repairs are delayed. In such

scenarios, LBS users utilize their real locations as a core element when issuing LBS queries. LBS recommendation systems respond according to the steps illustrated in Figure 1.

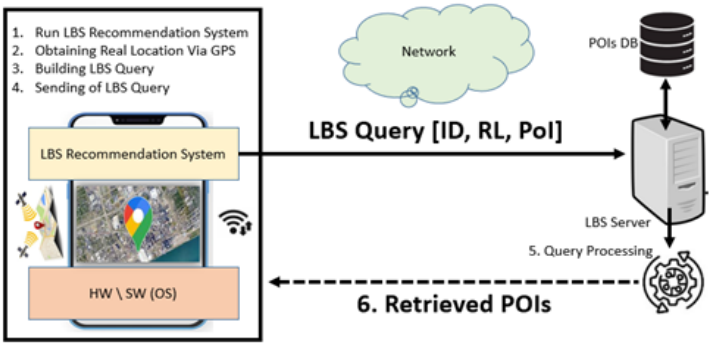

Figure 1. Using LBS recommendation systems

As shown in Figure 1, four main steps are performed at the LBS user including running the LBS application, which is already installed on the user's device, then the real location is obtained by GPS. The LBS query is issued from the user side based on the real location. The LBS query includes the identity of the user and the desired POI. On the LBS server side, the received LBS query is handled and the results found in the linked POI dataset are returned back to the user. However, from the perspective of a user who has concerns about privacy, Figure 1 uncovers a critical issue related to revealing their real location, it being tracked, and then a malicious profile created by an attacker. Research such as [3], [4], [5] has proposed ways to protect the location privacy of LBS recommendation systems, all with the aim of achieving the target of a higher degree of privacy protection. However, none of these works employed advanced techniques such as deep learning (DL) to enhance the privacy protection level. Employing DL techniques such as long short-term memory (LSTM) enhances the privacy protection level. That is because the data used to query a POI form trajectories that reflect the LBS behavior, and such data falls under a time series data type that suits the environment of the LSTM technique [6].

Consider an attacker that aims to collect personal information about an LBS user. Collecting personal information can leads to revealing sensitive aspects of LBS users, such as his/her habits, customs, medical records or political leanings. The collected information can be exploited later to hurt the LBS user in their workplace (for example, informing the manager of the LBS user about the medical reports that may lead to make a decision of not promotion of the LBS user to a higher position). The attacker can achieve this malicious result by tracking the real location of the LBS user or analyzing the send queries [7], [8]. The probability of achieving a malicious goal is limited if the attacker uses a man-in-the-middle attack, as this requires the use of advanced methods to eavesdrop on the network and to gain unauthorized access to the LBS server. In the case that the attacker is the LBS server itself (or its maintainer), the probability of achieving the malicious target is high as all information stored on the LBS server is easy to obtain. Figure 2 illustrates the problem.

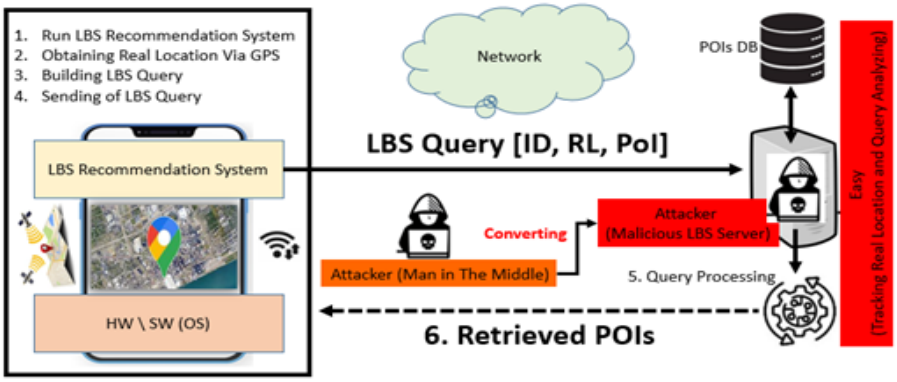

Figure 2. Problem of dealing with the LBS server as an attacker

Obtaining personal information about a victim (the LBS user) is easy if the LBS server acts as a malicious party, where tracking the real location for a series of requests (or queries) sent from the user's side or analyzing queries themselves strengthens the ability of the attacker to create a strong malicious profile. As a result, protection of LBS users against the malicious actions of untrusted LBS server is critical.

In responding to this problem, dummy-based approaches have been proposed, such as [9], [10]. The key idea of dummy-based approaches is to protect the real location of the LBS user by using false locations called dummies. This way leads to confusing the LBS server about determining the real location among the dummies. Dummy-based approaches start with determining the desirable privacy protection level modeled as $K-anonymity$, which is a common concept in privacy protection approaches, generating $(K-1)$ dummies, then creating (K) LBS queries based on both the real location and the generated dummies. The confusion occurs on the attacker's side (the malicious LBS server) when receiving all sent queries together as a package, where the probability of recognizing the real location among dummies is low. Figure 3 illustrates the key idea of dummy-based approaches.

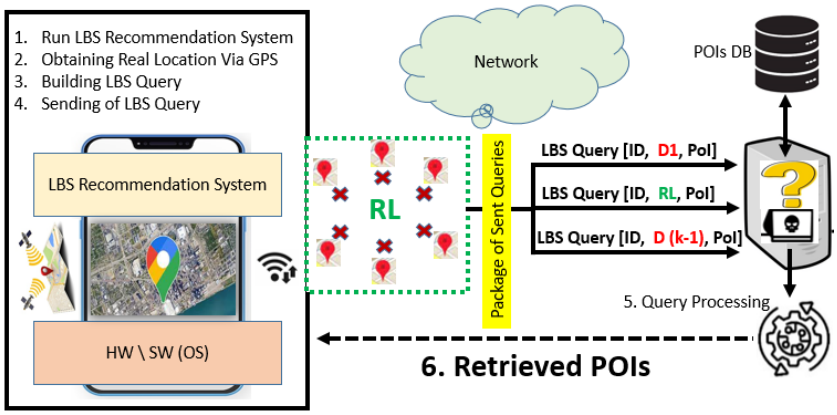

Figure 3. Key idea of dummy-based approaches

Figure 3 shows the following limitations:

1. Using the same POIs in all queries included in the package allows the LBS server (attacker) to apply query analyzing to extract personal information. This can be done by linking ID with POIs. For example, the attacker can infer that LBS user has a health problem when all POIs refer to one or more medical centers. This means that query privacy is not ensured even though the location privacy is protected by dummies [11].
2. The LBS server (attacker) can apply inference attacks, such as a location homogeneity attack and semantic location attack [12], to infer personal information that will be exploited to strengthen the malicious profile.
3. No DL technique is employed to generate strong dummies to maximize the privacy protection degree.

The limitations mentioned above form the space of the problem that is converted into research questions, as described below.

This study addresses the following research questions derived from the space of the problem:

1. How can LBS users ensure comprehensive privacy protection (i.e., both location and query privacy)?
2. How can LBS users ensure resistance against inference attacks (location homogeneity, semantic location, and query analysis attacks) against a malicious LBS server?
3. How can LBS user harness deep-learning techniques to maximize the privacy protection degree?

In addressing the research questions listed above, this study provides the following contributions:

- Regarding Research Question 1, an Intelligent Comprehensive Privacy Protection (IntCPP) system is proposed, where location privacy protection is achieved based on the intelligent generation of dummies

similar to real ones while query privacy protection is achieved by employing a 3-DES encryption algorithm.

- Regarding Research Question 2, resistance against both location homogeneity and semantic location attacks is achieved by the wise selection of final dummies from synthetic trajectories, while resistance against query analyzing attacks is achieved by building dummy queries accompanied by the masked identity of LBS users.
- Regarding Research Question 2, the LSTM technique is trained on a time-series-based dataset with an efficient pre-processing stage to generate dummy trajectories.

The rest of this paper is structured as follows: Section 2 presents deep-learning-based related works proposed previously to ensure privacy protection. In Section 3, the proposed deep-learning-based system is presented in detail. The experimental results are recorded and discussed along with security analysis in Section 4 and, finally, Section 5 concludes the study.

2. Related work

Many systematic review-based works have addressed privacy protection issues in LBS recommendation systems, such as [13], while others have addressed potential attacks that may be applied by attackers to break privacy protection approaches, such as [14]. This study classifies privacy protection approaches into traditional approaches (i.e., no intelligence-based techniques are used) and intelligent approaches. Figure 4 illustrates the classification of privacy protection approaches in this study.

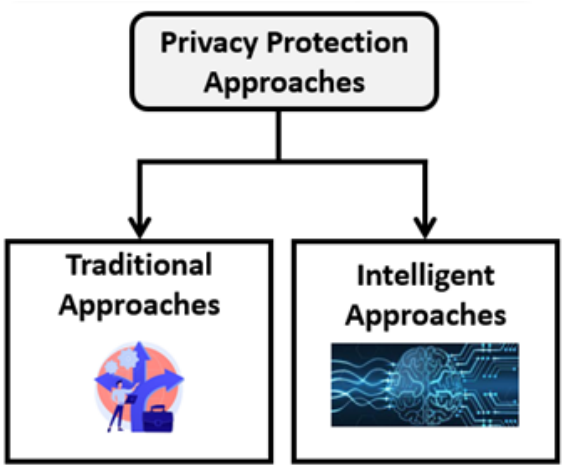

Figure 4. Classes of privacy protection approaches

2.1. Traditional approaches

There is a wide spectrum of traditional approaches proposed previously for privacy protection in LBS recommendation systems, such as mixzones [15], encryption-based approaches [16], transformation-based approaches [17], differential privacy approaches [18], and cache-based approaches [19]. None of these approaches relies on the dummy concept. Therefore, in this category, we briefly reviewed some of traditional dummy-based approaches only and let readers to go back the references of other approaches for more exploration.

In [20], dummy-based techniques are employed to safeguard the location privacy of LBS users, utilizing two distinct dummy generation approaches. The first, CirDummy, creates dummies by forming a virtual circle around the user's real location, while the second, GridDummy, generates dummies using a virtual grid encompassing the user's position. Meanwhile, [21] introduces the Destination Exchange (Dest-Ex) method, which leverages the historical motion trajectories of LBS users to produce dummies. To enhance robustness,

Dest-Ex specifically selects past trajectories that intersect with the user's current path. Another approach that uses dummies integrated with cache is provided in [22], where authors proposed two algorithms. The first algorithm is called the Caching-Aware Double Dummy Selection (CaDDSL), where the key idea is to generate dummies relying on selection of suitable false locations based on query probability (i.e., the real location and all selected dummies have the same query probability) and based on the maximum contribution to the cache. The final goal of the CaDDSL algorithm is to avoid connecting to the untrusted LBS provider and ensuring high resistance against inference attacks. The second algorithm is the Cache-Aware Overhead-Aware Dummy Selection (CaOaDSL), which is considered as an enhancement of the CaDDSL. The final goal of the CaOaDSL is to reduce the overhead on the network by employing agent-based software technology.

It is worth mentioning that all dummy-based approaches reviewed above are involved in the comparison to the proposed system of this study.

2.2. Intelligent approaches

In this category, privacy protection approaches that employ intelligent techniques are reviewed, noticing that there are a few approaches have been provided according to our investigation and to the best of our knowledge.

In [23], authors presented a new framework for location privacy protection using federated learning integrated with differential privacy. The framework is applied on the Internet of Vehicles (IoV), which uses location-based services. The key idea of location privacy protection is to deal with a privacy manager, as a global intelligent model, that is trained on the SUMO tool. A privacy manager adds noises to the paths of the vehicles with different degrees that act as dummies to confuse attackers. The authors stated that they achieved 15% improvement in the location privacy, where the actual accuracy obtained is 84%. For the purpose of comparison with our proposed system, we call this work as F-Fede-L for short.

The authors [24] proposed a deep learning-based system for location privacy protection in IoT-based applications that depends on LBS. The system performs a method called CNN-VoP. In their proposed architecture, the key element is a smart finder that searches for strong dummies in an intelligent way. The smart finder is trained on the Brightkite dataset using convolutional neural network (CNN), where the key idea is to scan the region of the LBS users and extract features of the geographical map to generate and classify dummies into weak and strong dummies using the Sigmoid function adopted with a support vector machine (SVM). Based on the CNN and the vector of dummies generated by the SVM, the name of the method (i.e., CNN-VoP) is developed, where VoP stands for Vector of Protection. The authors state that the achieved accuracy of classification of dummies is 99%. The CNN-VoP is involved later in the comparison with our proposed system in the evaluation section.

3. Proposed system

This section presents the proposed intelligent privacy protection system. Firstly, the framework of the system is presented. Then, a danger model that threatens the privacy protection offered by the proposed system is provided. Based on the danger model, the architecture of the proposed system is developed, where problem–solution-based methodology is used to present the architecture. The proposed system is called IntCPP, which stands for Intelligent Comprehensive Privacy Protection.

3.1. Framework of the IntCPP System

In this study, the framework represents the environment within which the IntCPP system operates. It includes a number of LBS users that hold mobiles with LBS recommendation systems, and the LBS users are located in a region that contain many PoIs. Each LBS user has a behavior inspired by her/his daily activities during the use of LBS recommendation systems. A specific dataset that contains daily activities is used to train the IntCPP system.

3.2. Danger model

Figure 5 presents the danger model, which has three pillars.

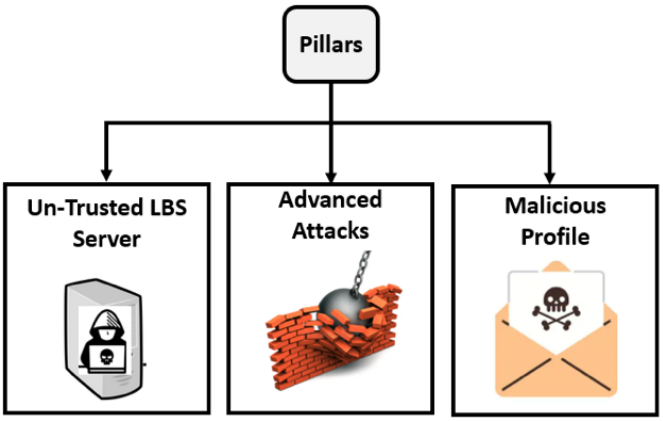

Figure 5. Pillars of the danger model

As illustrated in Figure 5, the IntCPP system is threatened by a danger model according to the following description:

1. An untrusted LBS server is the attacker (malicious party).
2. The attacker harnesses their knowledge about the geographical map of the rejoin form to which LBS queries are sent to break down the IntCPP system. This can be achieved by launching advanced attacks against location privacy (location homogeneity attacks and semantic location attacks) or against query privacy (query analyzing attacks).
3. Breaking down the IntCPP system opens the door to tracking the real location or analyzing the sent queries,and consequently collecting personal information and arranging it within a malicious profile.

3.3. The IntCPP system architecture

In this study, we use the architecture of the system proposed in [22], which is shown in Figure 6.

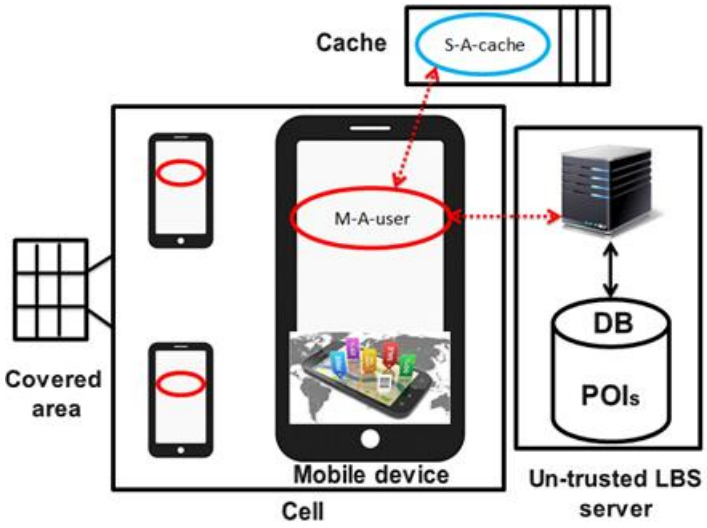

Figure 6. Architecture of system provided in [22]

In [22], the mobile agent (M-A-User) migrates either to the cache or to the untrusted LBS server to protect their location privacy by executing the CaOaDSL method. However, the mobile agent (M-A-User) does not use any deep-learning technique in the process of generating dummies when migrating to the untrusted LBS server (i.e., in case that no answer to the LBS query is found in the cache). In addition, it ensures only location privacy while query privacy is not (i.e., the attacker still has the ability to analyze LBS queries by linking the ID of the

LBS user and the wanted PoIs to collect personal information). The proposed IntCPP system enhances the role of the mobile agent (M-A-User) by using a DL technique (LSTM).

3.4. Role of the intelligent M-A-user agent in the IntCPP system

In general, DL-based systems are developed based on two steps: (1) model construction and (2) model usage. In this context, the model is the agent itself. In the first step, the agent is trained and tested, while in the second step the agent is used in reality, after achieving an acceptable accuracy level to protect the privacy of LBS users during testing in the first step.

The construction process of an intelligent M-A-User agent basically depends on employing the LSTM technique. This work uses a problem–solution-based approach in a cumulative way for the development of an intelligent M-A-User agent's role, as shown in Figure 7.

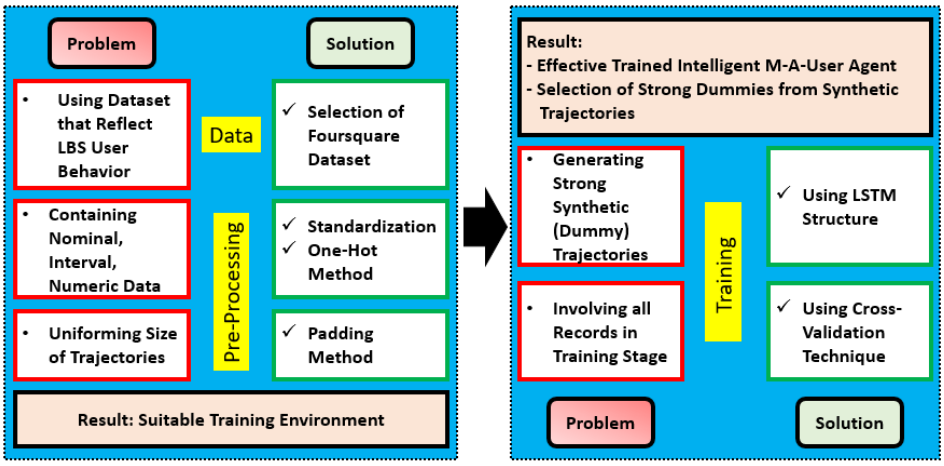

Figure 7. Problem–solution approach

As shown in Figure 7, there are many problems related to ensuring a suitable training environment and the effective training of the intelligent agent. Since this work aims to add the intelligence attribute to the privacy protection system, Figure 7 is converted into specific steps within the DL space through Figure 8.

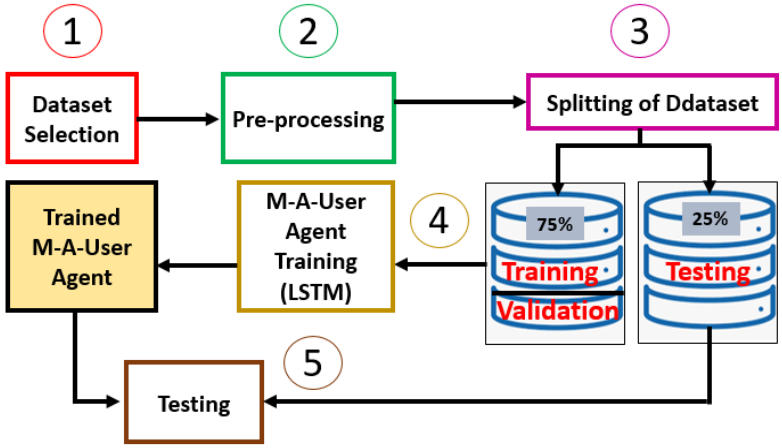

Figure 8. Steps within the DL space

3.4.1. Dataset selection

The M-A-User agent is trained on the Foursquare weekly trajectory dataset [25]. The reason behind selecting this dataset is that it reflects the behaviors of LBS users while performing daily activities in searching for PoI. The reflection of behaviors is inspired by the attributes of the dataset. Specifically, the behaviors of LBS users are represented by the identity of the LBS user, the identity of the shaped trajectory, location information of trajectories through points of both latitudes and longitudes over trajectories, detailed time information on

performing activities in both day and hour dimensions, and the category of PoI the LBS users search for. Such dataset falls under a time-series type, which is suitable for training an LSTM-based agent. Table 1 provides detailed description of attributes of the Foursquare weekly trajectory dataset.

Table 1. Description of foursquare weekly trajectory dataset

Attribute		Type	Range/Instance	Size
LBS user ID		Nominal	[1, 2, …]	193
Trajectory ID		Nominal	129	3079
Location information	Latitude	Interval	38.7423	66962
	Longitude	Interval	-90.3658	
Time information	Day	Nominal	[Sat, Sun, …, Frid]	7
	Hours	Numeric	[0, 2, …, 23]	24
PoI category		Nominal	[university, arts, …]	10

3.4.2. Data pre-processing

As summarized in Table 1, the attributes of the dataset belong to different types. The goal of the pre-processing step is to handle data to suit the environment of the LSTM, which consequently optimizes the training process and enhances the degree of accuracy. In this work, some attributes are kept un-touched (i.e., not involved in the handling process) and others undergo the handling process. The attributes that undergo the handling process result in a problem, as illustrated in Figure 9.

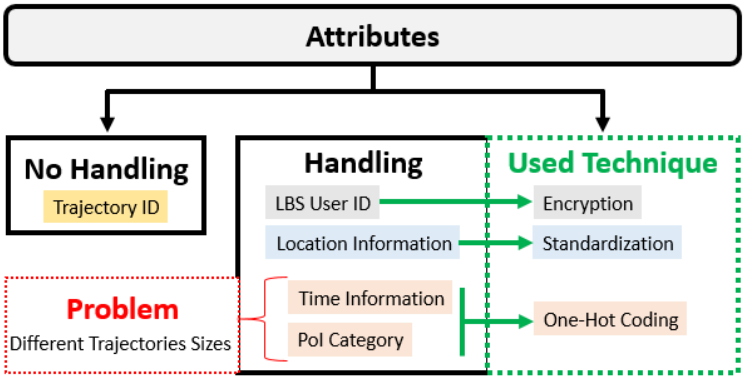

Figure 9. Techniques used in the pre-processing step

As shown in Figure 9, handling trajectory ID is out of process, as it reveals no personal information about the privacy of LBS users. Additionally, there are many techniques involved in the pre-processing step related to the rest of the attributes, as described in the following section.

3.4.2.1. Handling of LBS users' ID

Handling LBS users' ID is required to prevent the attacker from linking the user ID with the desired PoI. Linking the ID of the LBS user with the queried PoI is classified under malicious activities to extract/infer personal information about the LBS user for the purpose of enriching the malicious profile. Specifically, this malicious action helps the attacker to apply a query analyzing attack successfully. Therefore, hiding the LBS user's ID is necessary to prevent such malicious actions from the attacker. The hiding process uses encryption through the

3DES algorithm [26]. This in turn leads to ensuring query privacy because (1) the responses to the LBS queries basically depend on retrieving the queried PoI using unreadable code of the LBS user's ID and (2) even if the attacker tried to decrypt the code of LBS user's ID, failure is a natural result as the decryption key of 3DES algorithm is not shared and will be kept secret on the side of the LBS user. Thus, defending against a query-analyzing attack is ensured, as illustrated in Figure 10.

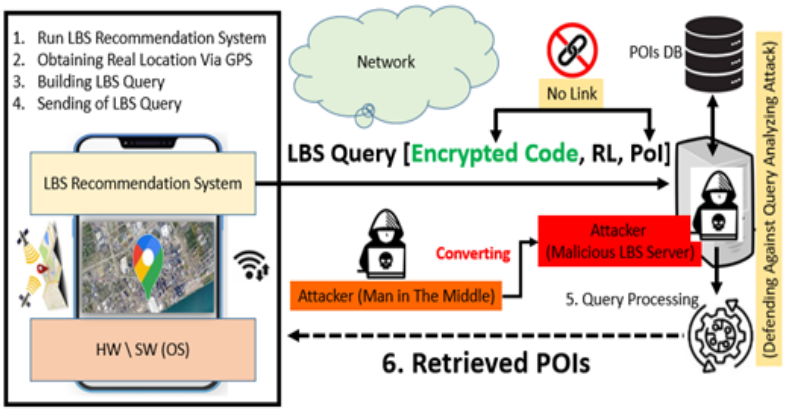

Figure 10. Defending against a query-analyzing attack

3.4.2.2. Handling of location information

Since the location information, represented by latitude and longitude, is of an interval type, it reflects a kind of noise. This in turn negatively affects the training process and results in a deteriorating accuracy level. In responding to this issue, a smoothing tactic is used. In this work, the smoothing tactic relies on a standardization method. The key idea is to determine the centroid of each trajectory and then calculate the deviations of the points. After smoothing the location information using a standardization technique, all latitudes and longitudes of all queried PoIs will be cleaned and of numeric type. This fits the environment of the LSTM method and contributes to enhancing the learning process.

3.4.2.3. Handling of both time information and PoI category

Handling the time information is performed based on the one-hot method (OHM) [27]. The key idea behind the OHM is representing data using a victor of binary bits ($K \in \{0,1\}^N$) according to the following formula:

$$K_i = \begin{cases} 1, if\ x = i \\ 0, otherwise \end{cases} for\ i = 1, 2, 3, \dots, N \qquad (1)$$

Where:

N : Possible options.

x : Certain variables from the available set (days/hours or PoI category).

Figure 11 illustrates the implementation of the OHM on the query "Searching for a university on Sunday@5 PM".

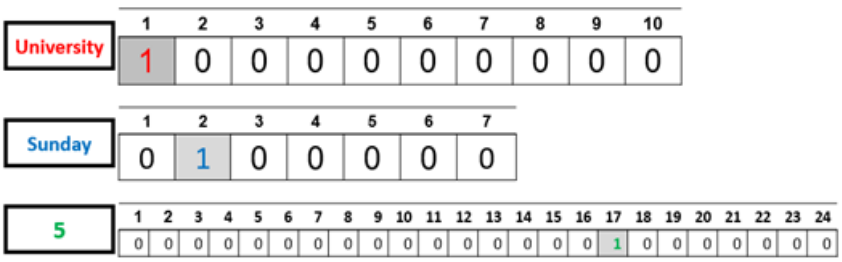

Figure 11. Example of implementation of thevOHM

As shown in Figure 11, for POIs, there are 10, 7, and 24 rooms in the three binary vectors for PoI, days, and hours, respectively. When an LBS user issues a query searching for a university on Sunday@5 PM, the output of the OHM is a three binary-vectors for each attribute according to the following description:

- The first room of the first vector is filled by "1".
- The second room of the second vector is filled by "1".
- The 17th room of the third vector is filled by "1".
- The rest of the rooms in all vectors are filled by "0".

3.4.2.4. Problem associated with implementation of OHM

However, implementing of OHM leads to a problem of different trajectories sizes, as the number of queried PoIs differs from one trajectory to another. This problem is explained by the following scenario:

1. For a certain activity, the LBS user may query about three PoIs. This means that when applying the OHM, the number of rooms (i.e., the size of the first trajectory) will be 3 (PoI) × (10 + 7 + 24) = 123.
2. For a different activity, the LBS user may query about two PoI. This means that when applying the OHM, the number of rooms (i.e., the size of the second trajectory) will be 2 (PoI) × (10 + 7 + 24) = 82.

It is obvious that the representations of trajectories differ in terms of size. This is because the trajectory size functions based on the number of involved PoIs within the activity.

3.4.2.5. Padding-based Solution

To solve this problem, the padding method is used [28]. The key idea of the padding method is to add zeros to adjust the size of trajectories. In this work, in the case of existing different trajectories, the padding method takes into consideration the longest trajectory to adjust the size of smaller trajectories so that all of them will be of the same size. As an implementation of a padding-based solution to the problem presented in the afore-mentioned scenario, the following steps are performed:

1. Difference between the size of the first trajectory and the second one is calculated (123 – 82 = 41).
2. Adding 41 rooms of "0" values to the second trajectory.

3.4.3. Splitting of the dataset

In the context of developing DL-based systems, splitting dataset can be performed based on the holdout approach [29]. The key idea of this approach is to divide the dataset into training and testing parts used for training and testing, respectively (for example, 25% and 75%), as shown in Figure 12.

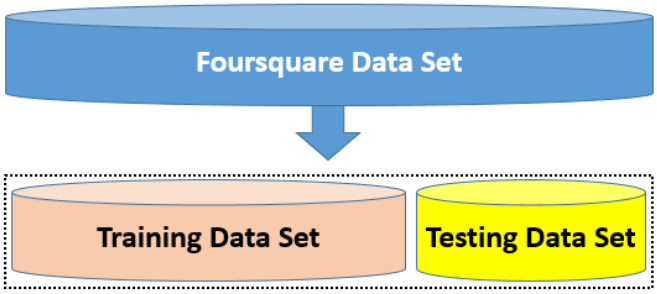

Figure 12. Key idea of the holdout approach

However, the holdout approach suffers from the following limitations [30]:

1. It arbitrarily divides the dataset into training and testing parts, which are independent from each other;
2. In-dependency leads to ignoring important features of data during the training stage as the testing data are not involved in the training stage. This leads to confusion in the training stage in terms of obtaining highest level of accuracy; and

3. It may lead to a model configuration-based problem during the training stage. That is because sometimes the training of a model may reach a high level of complexity, which results in infeasible training. Therefore, a validation part must be involved in the splitting process.

The limitations of the holdout approach lead to unstable training, which negatively affects the degree of accuracy. In responding to these limitations, this work uses the cross-validation method (CVM), which has been proven to enhance the training process, and consequently the accuracy level. Figure 13 illustrates the concept of the CVM.

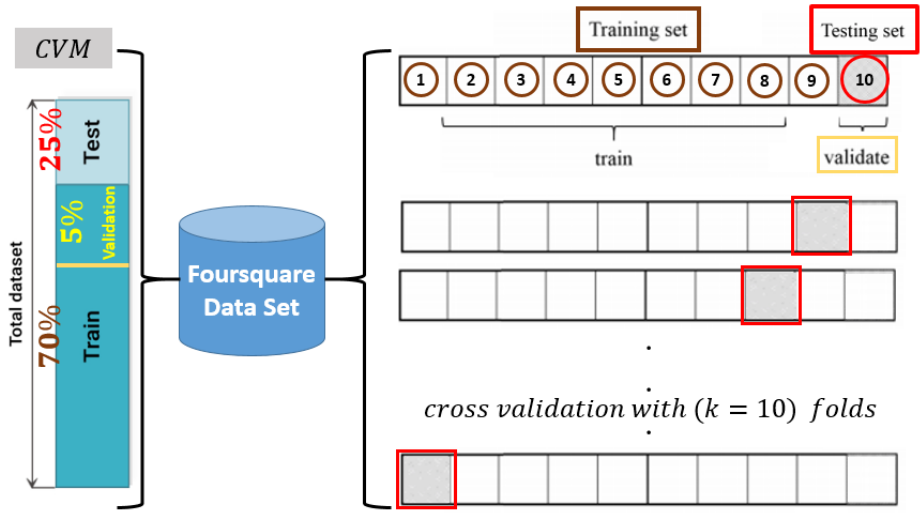

Figure 13. Concept of the CVM

As shown in Figure 13, the CVM is configured by (k=10), which means that the dataset is divided into 10 folds. In iteration one, the 10th fold is used to validate and test the model while the remaining folds are used for training. The same scenario is repeated taking into account changing the location of the validation/testing fold in a diagonal manner. This ensures all records of the dataset are covered without ignoring any useful information during the training stage, which leads to a stable training process.

3.4.4. Training of the M-A-User agent

After performing the pre-processing and splitting processes, the M-A-User agent will be ready to gain the intelligence feature (i.e., training). The technique that is used in this work is the LSTM. The input of the LSTM is a real trajectory, while the output is a dummy trajectory that cannot be distinguished from the real one. Figure 14 illustrates the structure of the LSTM used in this work.

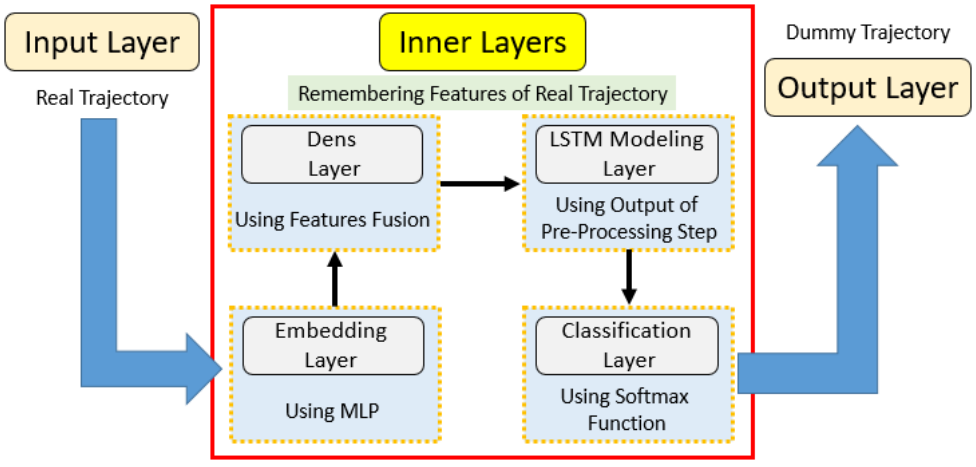

Figure 14. Structure of the LSTM technique

As shown in Figure 14, there are six layers involved in the LSTM structure. The input layer receives the real trajectory. The inner layers are responsible for implementing the key principle of the LSTM technique, which is remembering the previous information (i.e., the data of real trajectory) though the forget gate, and based on the remembered data a new data is generated to shape/generate the dummy trajectory. In detail:

1. The embedding layer is responsible for embedding the spatial information (latitude and longitude deviations), the temporal information (day and hour), and PoI category using multilayer perceptrons (MLPs).
2. The dense layer is responsible for fusion of the embedded features.
3. The LSTM modeling layer is responsible for modeling the fused features to produce the corresponding vectors, taking into consideration the modeling used in the pre-processing step.
4. The classification layer is responsible for classifying the dummy trajectory if it is similar to the real one or not. This will be used for evaluation in the results and discussion section based on the accuracy measure.

The output layer includes the dummy trajectory. The generated dummy trajectory is shaped based on dummy locations. From the set of generated dummies that are included in the dummy trajectory, the M-A-User agent elects the actual dummies that will be used to ensure location privacy. However, when implementing the k-anonymity concept, not all dummies included in the dummy trajectory are strong and resistant against location homogeneity and semantic location attacks, as they may be near to each other. Therefore, the election process must be conducted wisely. In this work, the same criteria of election process used in [22] is adopted. Two main conditions are used to obtain the final strong dummies:

1. All final dummies have the same query probability as the real location; and
2. All final dummies are far away from each other.

Figure 15 illustrates how to elect the final dummies used to ensure location privacy by 4-privacy degree based on the k-anonymity concept.

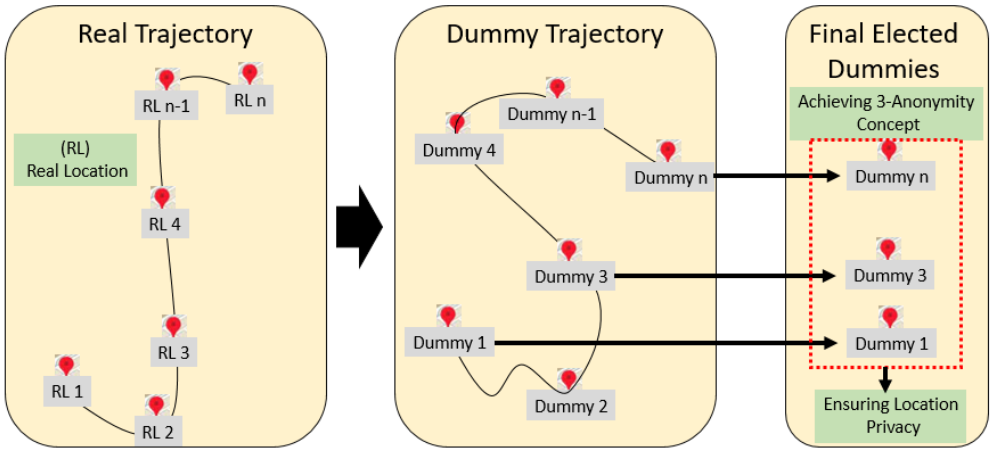

Figure 15. Obtaining the final dummy set from the dummy trajectory

Algorithm 1: Intelligent M-A-User Agent

Upload dataset
Initialize itinerary of agent
While (Dataset is not empty) do \\ Performing Pre-Processing
1 For (LBS user ID) do
2 Call 3-DES, Encrypt, and Update
3 For (Location Information) do
4 Call Standardization Method and Update

```
For (Time Information & PoI Category) do
Call OHM Method and Update
Return Cleaned Dataset
Call CVM (k=10) \\ Splitting of Dataset
    For (k =1, k <= 10, k ++) do \\ Training
        Call LSTM
            Train on all Iterations
            Obtain Dummy Trajectory
            Enter Desirable Level of Privacy
            Extract Set of Dummies
                If (Election Criteria is met) then
                Add Dummy to the Final Dummy Set
        End
Retrieve Final Dummy Set
End
```

If (condition) then

At this point, the M-A-User agent gains intelligence property to ensure comprehensive privacy protection (query privacy protection through the encryption of LBS user ID to prevent linking to the PoIs and location privacy protection through training of LSTM). Thus, the proposed IntCPP system is ready for testing. Algorithm 1 presents the pseudocode of the overall process of building the intelligent M-A-User agent.

3.4.5. Testing

Testing is used to evaluate the IntCPP system through measuring the performance of the intelligent M-A-User agent (using the data included in the testing part). Therefore, testing in this work refers to a comprehensive evaluation of the proposed IntCPP system. Comprehensive evaluation requires presenting the used measures. There are two kinds of measures in this work, as described in the following section.

3.4.5.1. Deep Learning-based measures

The most popular measure used in the DL domain is accuracy. Accuracy refers to how accurate the generated dummies are in comparison to real ones. Another common measure is the ROC curve, which is used to compare intelligent systems based on the area under the curve. For accuracy measure, it is inspired from the confusion matrix, which contains four main elements as summarized in Table 2.

Table 2. Confusion matrix

Generated Dummy / Actual Dummy	**DM**	**¬ DM**	**Sum**
DM	TP	FN	S
¬ DM	FP	TN	Su
Sum	ToDM	$\widetilde{T0DM}$	All

The elements of the confusion matrix are described as follows:

- True positives (TPs): The positive dummies that were correctly labeled as similar to real ones by the IntCPP system;
- True negatives (TNs): The negative dummies that were correctly labeled as dissimilar to real ones by the IntCPP system;
- False positives (FPs): The negative dummies that were incorrectly labeled as similar to real ones by the IntCPP system; and

- False negatives (FNs): The positive dummies that were incorrectly labeled as dissimilar to real ones by the IntCPP system

High accuracy is preferred as it indicates a high performance. Accuracy is given by

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{All}} \quad (2)$$

As for the ROC curve, it follows a special mechanism for the evaluation of two given systems. It first calculates the area under curve, then it represents this area in terms of true positive rate (vertical axis in the curve) and false positive rate (horizontal axis in the curve). Finally, the evaluation output relies on the statement "The closer to the diagonal line, the less accurate is the model".

3.4.5.2. Privacy protection-based measures

As this work is considered an optimization of our previous work [22] and to ensure the fair context of comparison, the same privacy measures are used.

Entropy is a measure used to quantify how confusion occurs on the side of the attacker when trying to determine the real location among dummies. It is given by

$$E = -\sum_{i=1}^{k} \acute{p}_i \times log_2(\acute{p}_i) \quad (3)$$

Where

k: Level of desirable K-anonymity level.

$\acute{p}_i$: Query probability.

Based on entropy, the amount of compromised privacy (ACP) measure is used. It is given by

$$\text{ACP} = \sum_{i=1}^{n}\left(\log_2(k) - E(t_n)\right), \text{where } t_n \in T \quad (4)$$

Where, $T = (t_1, t_2, t_3, \dots, t_n)$ refers to the moments at which the LBS user issues queries, where each query is protected by $k-1$ dummy locations. The ACP measure is used to evaluate the proposed IntCPP system under threats of attacks.

Cache hit ratio (CHR) represents the ratio of the number of queries answered by the cache to the total number of queries in the IntCPP system. It is given by:

$$CHR = \frac{|Q_{answered-cache}|}{|Q_{answered-cache}| + |Q_{answered-server}|} \quad (5)$$

4. Results ad security analysis discussion

This section is structured so that setup of the operational environment is presented firstly, followed by results and discussions related to providing evidence about resistance against attacks.

4.1. Setup

The same simulation used in our previous work [22] is employed to conduct experiments. The same parameter is used to configure simulation (i.e., 160×160 cells, and a total of 10,000 users). In addition, the same way to obtain query probabilities is used (i.e., using Google Maps API). Experiments are conducted on a machine with specifications shown in the following copy-screen Figure 16.

Figure 16. Copy-screen of machine specifications

In addition, the proposed IntCPP system is compared to the following approaches to prove its superiority: CaOaDSL, GridDummy, CirDummy, Dest-Ex, CNN-VoP, and Fed approaches.

4.2. Results and discussion

In round one of the IntCPP system evaluation, DL-based measures are used. In this context, the IntCPP system is compared to both the CNN-VoP and Fed approaches since they are built within the DL domain.

4.2.1. Deep learning-based evaluation

The IntCPP system is evaluated in comparison to both CNN-VoP and F-Fed-L in terms of accuracy, as shown in Figure 17.

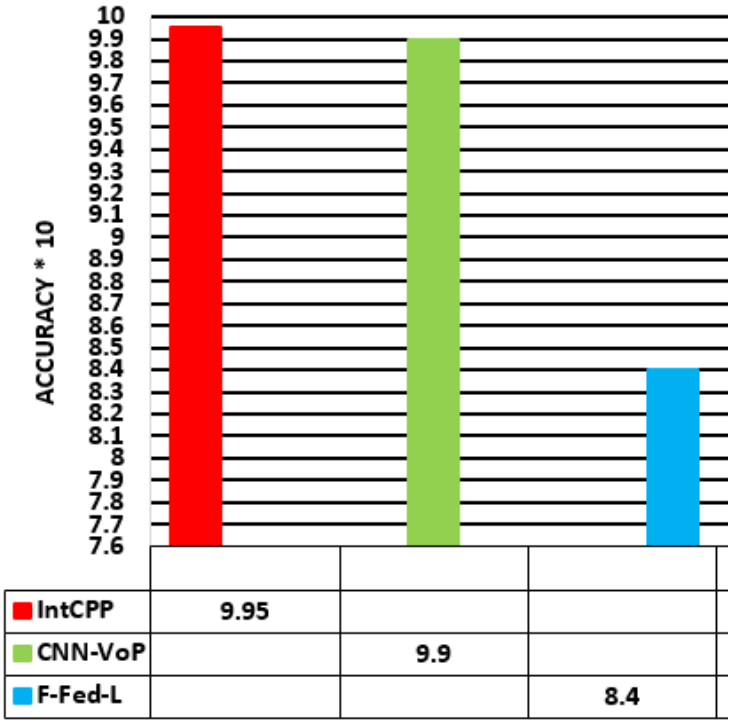

Figure 17. Accuracy-based evaluation

4.2.1.1. Discussion of the accuracy results

Figure 17 proves the superiority of our proposed IntCPP system. The results show that IntCPP achieves the highest accuracy (9.95 × 10 = 99.5 %), making it the best-performing system among the three. This superior performance indicates that similarity between dummies and real locations is high. That is because it employs the LSTM technique effectively to generate high-quality synthetic/dummy trajectories. Effective generated dummy trajectories is a result of good training on the used dataset, where pre-processing plays an important

role in obtaining patterns that represent the behaviors of LBS users and related features. Compared to CNN-VoP, the IntCPP system enhances accuracy by (0.05). This is because the CNN-VoP system depends on analyzing the geographical map of LBS users' locations to extract patterns of motions. Extracted patterns based on images of motions do not provide accurate details when compared to patterns extracted based on remembering historical trajectories. However, the CNN-VoP system is still a strong competitor to the IntCPP system as it provides accuracy close to the proposed system. Compared to the F-Fed-L system, the IntCPP system achieves better accuracy by (1.55) enhancement. That is because the F-Fed-L system completely ignores the trajectory details of vehicles, as it basically relies on the leader to manage the privacy. The leader uses various levels of noise to generate dummies, which are inaccurate in terms of generating false locations similar to the real ones. Consequently, the historical data of real trajectories are ignored since dummies are generated based on external noise that does not belong to the original locations. In contrast, the LSTM technique used by the IntCPP system takes into account details of the original trajectories, which leads to higher accuracy and reliability.

The IntCPP system is evaluated in comparison to both CNN-VoP and F-Fed-L in terms of the ROC curve, as shown in Figure 18.

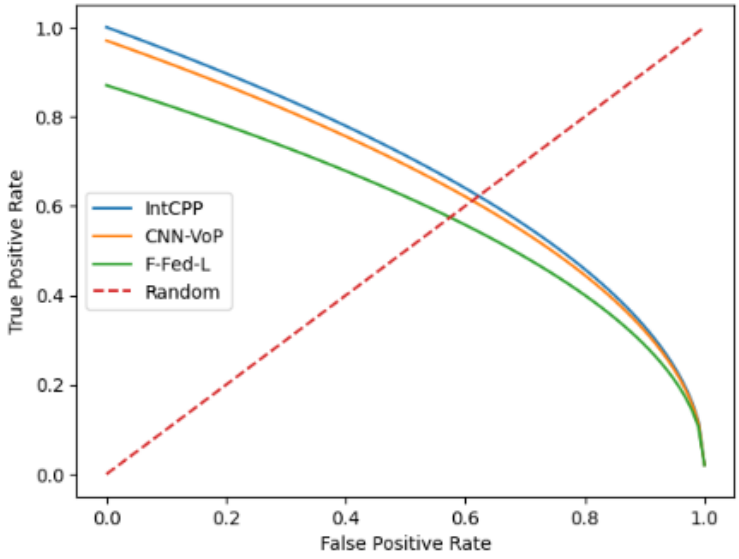

Figure 18. ROC curve-based evaluation

4.2.1.2. Discussion of the ROC curve results

Figure 18 shows the following facts, supporting the recorded results relying on accuracy measure:

1. For the IntCPP system, the curve is closest to the top-left corner, indicating the highest true positive rate (TPR) for a given false positive rate (FPR). This is consistent with its highest accuracy, obtained above, and implies the largest area under curve (AUC), which in turn means the strongest classification capability.
2. For the CNN-VoP system, the ROC curve lies just below IntCPP, showing very competitive performance. The small gap suggests that CNN-VoP has comparable feature-learning ability, but slightly less optimal decision boundaries compared to IntCPP.
3. For the F-Fed-L system, the corresponding curve is clearly lower than the other two, meaning that for the same FPR, it achieves a lower TPR. This aligns with its lower accuracy obtained above.

After providing evidence of superiority in terms of a DL-based domain, the IntCPP system is evaluated in the privacy-based domain.

4.2.2. Privacy-based evaluation

The IntCPP system is evaluated in comparison to CaOaDSL, CirDummy, GridDummy, and Dest-Ex systems in terms of entropy values, as shown in Figure 19.

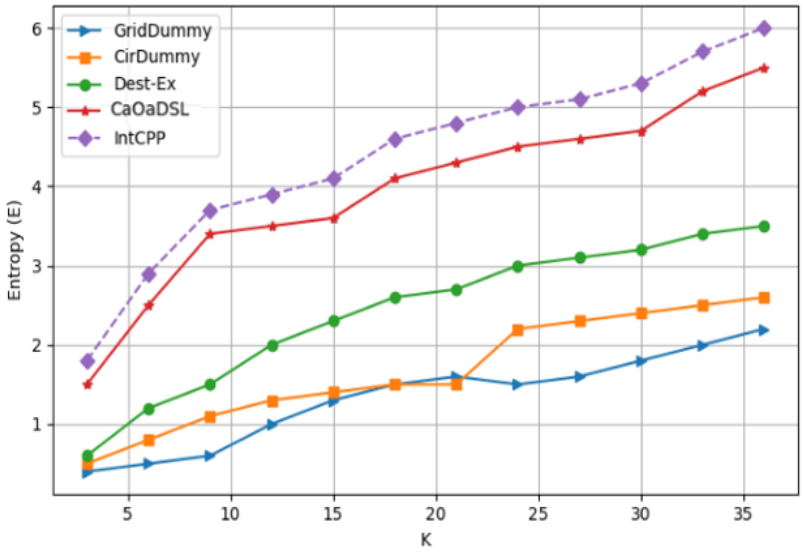

Figure 19. Entropy-based evaluation

Figure 19 shows the entropy values of the systems involved in the comparison when level of anonymity (K) increased within the range [3 to 36].

4.2.2.1. Discussion of entropy results

Figure 19 provides the second evidence of the superiority of the IntCPP system, sharing the following results:

1. Increasing the k value leads to increases in the value of E in all systems. This is a natural result when the LBS user wants to ensure a high level of location privacy protection.
2. For the IntCPP system, within the range $k \in [3-36]$, entropy records value within the range $E \in [1.8-6]$. Taking an average of E boundaries ($\frac{6-1.8}{2}$), the final E value is 2.1.
3. For the CaOaDSL system, within the range $k \in [3-36]$, entropy records value within the range $E \in [1.5-5]$. Depending on the average, the final E value is 2.
4. For the Dest-Ex system, within the range $k \in [3-36]$, entropy records value within the range $E \in [0.5-3.5]$. Depending on the average, the final E value is 1.5.
5. For the CirDummy system, within the range $k \in [3-36]$, entropy records value within the range $E \in [0.4-2.6]$. Depending on the average, the final E value is 1.1.
6. For the GridDummy system, within the range $k \in [3-36]$, entropy records value within the range $E \in [0.3-2.1]$. Depending on the average, the final E value is 0.9.

Table 3 summarizes the final entropy values with the measure of enhancement degree of the IntCPP system compared to other systems individually.

Table 3. Final values of achieved entropy

System	IntCPP	CaOaDSL	Dest-Ex	CirDummy	GridDummy
E Value	2.1	2	1.5	1.1	0.9
Enhancement		0.1	0.6	1	1.2
Cumulative enhancement	2.0				

The proposed IntCPP system achieves 0.1 enhancement for location privacy protection when compared to the CaOaDSL system. This enhancement is justified by employing the LSTM technique to generate dummy trajectories that lead to a preset set of dummies similar to real ones. However, the enhancement degree is small and justified by using the same criteria of dummy selection in both systems. Compared to the GridDummy system, which records the lowest level of location privacy protection, the IntCPP system achieves a 1.2 enhancement degree. That is because the GridDummy system does not use any intelligent method to generate dummy locations as well as mainly relying on limiting the space of dummies' generation within a specific grid without taking into consideration any criteria of selection.

The IntCPP system is evaluated in comparison to CaOaDSL, CirDummy, GridDummy, and Dest-Ex systems in terms of the ACP values, as shown in Figure 20.

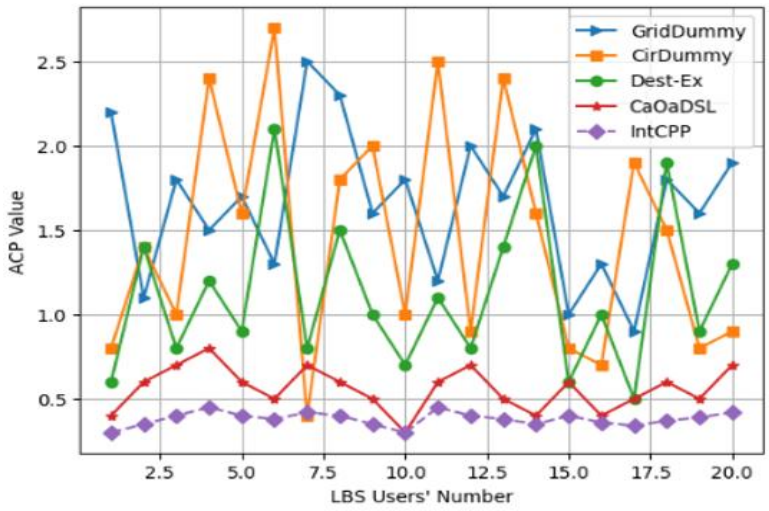

Figure 20. ACP-based evaluation under threats of both location homogeneity and semantic location attacks, risk threshold 0.5

4.2.2.2. Discussion of ACP results

Figure 20 provides the third evidence of the IntCPP's system superiority when using risk/entropy threshold of (0.5), stating the following results:

1. For the IntCPP system and under threat of both location homogeneity and semantic location attacks, the number of users that reach the danger level is the minimum when compared to the CaOaDSL system (the second ranked system in terms of resistance against attacks).
2. The rate of users who reached the risk threshold is (0) in the IntCPP system, compared to (11, 18, 20, 20) for CaOaDSL, Dest-Ex, CirDummy, GridDummy systems, respectively.
3. Using risk threshold of (0.8) in our previous work [22] leads to (2 ACP value) of CaOaDSL, while increasing the level of protection by decreasing the risk threshold to (0.5) in this work leads to (11 ACP value). However, for the IntCPP system, the value of ACP is stable at (0), which reflects strong resistance against attacks. This is due to generating dummies based on the output of LSTM, which ensures that original trajectories are too similar to synthetic ones.

4.2.2.3. Resistance against inference attacks based on ACP results (security analyzing of location privacy)

Since both location homogeneity and semantic location attacks target location privacy, a discussion of security analysis is provided under threats of both attacks. In this context, the following statements are provided:

1. We assume that the attacker is familiar with the intelligent way used to generate final dummies.
2. The attacker tries to infer the real location among final set of dummies using both attacks.

3. Since the generated dummies are very similar to real ones in terms of features and query probability, the attacker is confused in determining the real location among dummies.
4. Since the size of the final set of dummies (i.e., the number of dummies included in the final set) is bigger than the size of the actual set of dummies (i.e., the number of dummies that are actually used to achieve certain k-anonymity/privacy protection levels), the attacker is forced to guess the real location randomly without any degree of certainty. This means no feasibility is gained, which reflects the failure of attacks and a high corresponding resistance.

4.2.2.4. Resistance against inference attacks based on ACP results (security analyzing of query privacy)

Since query-analyzing attacks target query privacy, discussion of the security analysis is provided under threats of this attack. In this context, the number of LBS users that reach a danger level is calculated, as illustrated in Figure 21.

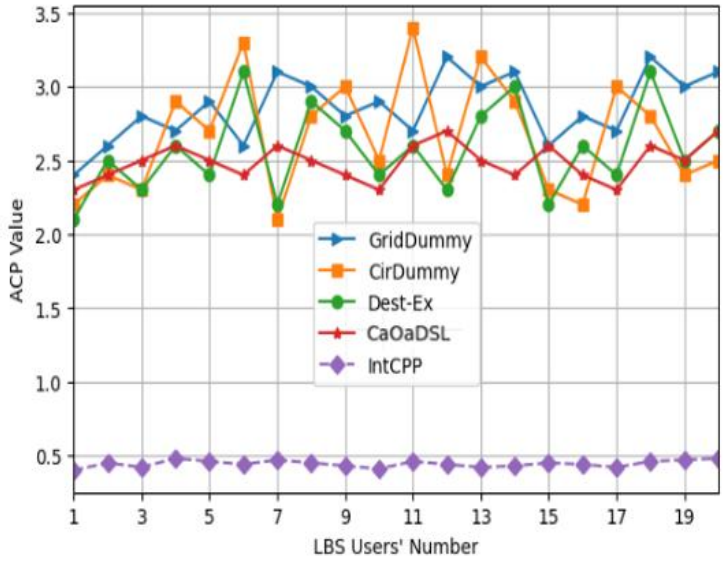

Figure 21. ACP-based evaluation under threat of query analyzing attack, risk threshold 0.5

Figure 21 shows that the number of LBS users who reach the danger level is zero (ACP = 0) in the IntCPP system, while all LBS users are within the risk area for all other systems. This means that the proposed IntCPP system achieves the highest resistance against query analyzing attacks. In the context of security analyzing against this attack, the following statements are provided:

1. We assume that the attacker pays significant attention to the link ID of the LBS user with the queried PoIs.
2. The attacker tries to infer personal information by applying query-analyzing attacks on real sent queries.
3. Since the queries are sent as a package (i.e., the query that is constructed based on the real location and queries that are constructed based on the dummy locations), the real query will be hidden within the group of dummy queries. This means that query privacy is achieved in terms of dummies.
4. Encrypting the ID of the LBS user leads to providing a new unreadable ID, which can be treated as dummy to the original ID. Thus, the sent package will contain dummy locations and a dummy ID of the LBS user.
5. The attacker tries to decrypt the unreadable ID first and then to link the correct ID to the queried PoIs to benefit from the query analyzing attack. Even if the decryption process occurs within the room of the attacker, obtaining the correct ID is hard as the decryption key of the 3DES algorithm is kept secret on the side of the LBS user.

6. Obtaining only queried PoIs without real ID is unfeasible when applying query analyzing attacks as the linking process will be between obvious PoIs and un-defined IDs. Therefore, the only choice of the attacker is to guess the real query randomly, resulting in confusion. This means that the query analyzing attack will not succeed and query privacy protection is ensured.

The IntCPP system is evaluated in comparison to the CaOaDSL, CirDummy, GridDummy, and Dest-Ex systems in terms of CHR values, as shown in Figure 22.

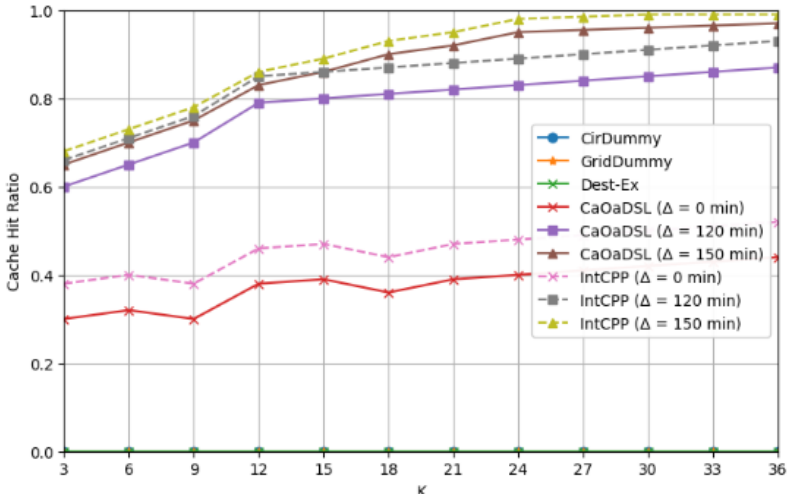

Figure 22. CHR-based evaluation

4.2.2.5. Discussion of the CHR results

Figure 22 provides the fourth evidence of IntCPP system's superiority when taking the values of the CHR under different snapshots of simulation ($\Delta = 0, 120, 150$), stating the following results:

1. In contrast to the CirDummy, GridDummy, and Dest-Ex systems, where the CHR is always zero, as they do not employ the caching concept, the IntCPP and CaOaDSL systems record increasing the CHR values over the taken snapshots.
2. The enhancement scores of the CHR achieved by the IntCPP system are summarized in Table 4:

Table 4. Enhancement scores

System	**Boundary**	**Snapshots**		
		$\Delta = 0$	**$\Delta = 120$**	**$\Delta = 150$**
IntCPP	*Lower boundary of CHR*	0.38	0.62	0.69
CaOaDSL	*Lower boundary of CHR*	0.3	0.6	0.62
Enhancement degree		**0.08**	**0.02**	**0.07**
IntCPP	*Higher boundary of CHR*	0.5	0.95	0.99
CaOaDSL	*Higher boundary of CHR*	0.42	0.9	0.95
Enhancement degree		**0.08**	**0.05**	**0.04**
AVG cumulative enhancement		**0.17**		

In general, the data recorded in Table 4 shows that the CHR values increase for the two systems as the value of Δ increases. Moreover, the CHR values of both lower and higher boundaries of the IntCPP system are higher than of the CaOaDSL system, reflecting a general enhancement in CHR values when using the IntCPP system. However, enhancement remains constant in the first snapshot at 0.08. That is because the contribution of dummies is a function of time as the content of the cache (i.e., the results of answered queries) is empty when starting the simulation. Over time and meeting the second snapshot, the cache starts to store results that can be used to answer future queries, achieving 0.02 and 0.05 enhancement degrees for lower and higher boundaries, respectively. As for the third snapshot, the corresponding enhancement degree is 0.07 and 0.04. This enhancement is a result of using the LSTM technique to generate dummies that retrieve the most adopted PoIs to the daily/natural behavior of LBS users. In contrast to the IntCPP system, the CaOaDSL system ignores the behavior of LBS users completely.

5. Conclusion

Ensuring comprehensive privacy protection (location privacy and query privacy) of location-based services is a top requirement to increase the trust of users when searching for points of interests. Works have proposed previously employed intelligent methods to enhance privacy protection. Motivated by this statement, the IntCPP system is proposed in this work. This work is considered as an optimization of our previous work by employing deep learning to enhance privacy protection levels. The IntCPP system is trained using the LSTM deep learning technique. The selected dataset, Foursquare weekly trajectory, undergoes an effective pre-processing stage to prepare a suitable environment to train the LSTM. A problem–solution-based approach is followed to achieve this target, where a standardization method is used to deal with the noise of location information issue, one-hot method is used to deal with the categorical data issue, and a padding-based method is used to deal with the various lengths of the trajectories. A cross-validation method is employed to obtain training and testing parts in responding to the features loss issue. After obtaining the trained model, the M-A-User agent carries this intelligent model to be its main task when reaching the destination (the malicious LBS server). Synthetic trajectories similar to real ones are generated by the LSTM-based model, containing strong dummies. Among the generated dummies, the most resistant dummies are elected to ensure resistance against location homogeneity and semantic location attacks, ensuring location privacy. To ensure query privacy as well as high resistance against query analyzing attacks, the link between the identity of the LBS user and queried PoIs is cut through encrypting identities. The results of the IntCPP system evaluation showed superiority when compared to similar systems in terms of accuracy, the ROC curve, entropy, and the amount of compromised privacy measures. This work provides a proof that the privacy protection of LBS can be enhanced by harnessing deep learning to generate strong dummies.

However, limitations of this work are related to using one dataset for training and ignoring both the security of agents and computational complexity. In future works, we intend to handle such limitations to make the system more reliable in realistic usage.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Author contribution

The contribution to the paper is as follows: Omar F. Aloufi: study conception and design; Omar F. Aloufi: data collection; Omar F. Aloufi: analysis and interpretation of results; Omar F. Aloufi: methodology development; Omar F. Aloufi: draft preparation; Ahmed S. Alfakeeh, Fahad M. Alotaibi, Samah A. Abbas:

critical revision of the manuscript for important intellectual content. All authors approved the final version of the manuscript.

References

[1] H. M. Ibrahim, "Artificial Intelligence (AI) and Internet of Things (IoT) Applications in Smart Cities: Literature Review," *Iraqi Journal for Computers and Informatics,* vol. 52, no. 1, pp. 35-53, 2026, https://doi.org/10.25195/ijci.v52i1.573.

[2] E. Hasan, M. Rahman, C. Ding, J. X. Huang, and S. Raza, "Based recommender systems: a survey of approaches, challenges and future perspectives," *ACM Computing Surveys,* vol. 58, no. 1, pp. 1-41, 2025, https://doi.org/10.1145/3742421.

[3] B. Liu, W. Zhou, T. Zhu, L. Gao, and Y. Xiang, "Location privacy and its applications: A systematic study," *IEEE access,* vol. 6, pp. 17606-17624, 2018, https://doi.org/10.1109/ACCESS.2018.2822260.

[4] H. Wang, R. Guan, P. Liu, and K. Liu, "OPSA-DP: A Trajectory Privacy Protection Scheme Based on the Optimal Decision-making of Obfuscation Points," *Computers & Security,* p. 104843, 2026, https://doi.org/10.1016/j.cose.2026.104843.

[5] X. Zhang, L. Gong, and S. Pu, "Location Privacy Protection Scheme Based on Secret State Computation for Randomization," *International Journal of Network Security,* vol. 28, no. 1, pp. 80-88, 2026, https://doi.org/10.6633/IJNS.202601_28(1).08.

[6] H. Wang *et al.*, "A time-series-based model to detect homogeneous regions of residents' dynamic living habits," *Geo-Spatial Information Science,* vol. 28, no. 4, pp. 1789-1806, 2025, https://doi.org/10.1080/10095020.2024.2437254.

[7] M. S. Alrahhal, M. Khemakhem, and K. Jambi, "A survey on privacy of location-based services: classification, inference attacks, and challenges," *Journal of Theoretical & Applied Information Technology,* vol. 95, no. 24, 2017.

[8] H. Alrahhal, M. S. Alrahhal, R. Jamous, and K. Jambi, "A symbiotic relationship based leader approach for privacy protection in location based services," *ISPRS International Journal of Geo-Information,* vol. 9, no. 6, p. 408, 2020, https://doi.org/10.3390/ijgi9060408.

[9] M. Dong *et al.*, "Dummy-Trajectory Synthesis: A Privacy-Preserving Approach for Semantic Trajectory Data in IoT-Based LBSN," *IEEE Internet of Things Journal,* 2025, https://doi.org/10.1109/JIOT.2025.3587442.

[10] L. Kuang, W. Shi, X. Chen, J. Zhang, and H. Liao, "A location semantic privacy protection model based on spatial influence," *Scientific reports,* vol. 15, no. 1, p. 15227, 2025, https://doi.org/10.1038/s41598-025-88553-9.

[11] G. Danqian, C. Li, C. Yu, M. Honglei, Z. Guoli, and D. Zhi, "Research on Joint Protection of LBS Location and Query Privacy in Internet of Vehicles Based on an Improved PIR Algorithm," *Concurrency and Computation: Practice and Experience,* vol. 37, no. 27-28, p. e70447, 2025, https://doi.org/10.1002/cpe.70447.

[12] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Personal and ubiquitous computing,* vol. 18, no. 1, pp. 163-175, 2014, https://doi.org/10.1007/s00779-012-0633-z.

[13] W. Huang, B. Liu, and H. Tang, "Privacy protection for recommendation system: a survey," in *Journal of Physics: Conference Series*, 2019, vol. 1325, no. 1: IOP Publishing, p. 012087, https://doi.org/10.1088/1742-6596/1325/1/012087.

[14] Y. Li *et al.*, "A scoping review of privacy protection in LBS: Architectures, Threats, and Defense mechanisms," *Journal of King Saud University Computer and Information Sciences,* vol. 37, no. 10, p. 315, 2025, https://doi.org/10.1007/s44443-025-00337-3.

[15] R. S. Zuberi and S. N. Ahmad, "Secure Mix-Zones for Privacy Protection of Road Network Location Based Services Users," *Journal of Computer Networks and Communications,* vol. 2016, no. 1, p. 3821593, 2016, https://doi.org/10.1155/2016/3821593.

[16] T. Feng, X. Wang, and X. Li, "LBS privacy protection technology based on searchable encryption mechanism," in *MATEC Web of Conferences*, 2018, vol. 189: EDP Sciences, p. 10013, https://doi.org/10.1051/matecconf/201818910013.

[17] D. Lin, E. Bertino, R. Cheng, and S. Prabhakar, "Position transformation: a location privacy protection method for moving objects," in *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*, 2008, pp. 62-71, https://doi.org/10.1145/1503402.1503414.

[18] B. Wang, H. Li, X. Ren, and Y. Guo, "An efficient differential privacy-based method for location privacy protection in location-based services," *Sensors,* vol. 23, no. 11, p. 5219, 2023, https://doi.org/10.3390/s23115219.

[19] Y. Cui *et al.*, "Cache-based privacy preserving solution for location and content protection in location-based services," *Sensors,* vol. 20, no. 16, p. 4651, 2020, https://doi.org/10.3390/s20164651.

[20] H. Lu, C. S. Jensen, and M. L. Yiu, "Pad: privacy-area aware, dummy-based location privacy in mobile services," in *Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access*, 2008, pp. 16-23, https://doi.org/10.1145/1626536.1626540.

[21] T. Hara, A. Suzuki, M. Iwata, Y. Arase, and X. Xie, "Dummy-based user location anonymization under real-world constraints," *Ieee Access,* vol. 4, pp. 673-687, 2016, https://doi.org/10.1109/ACCESS.2016.2526060.

[22] O. F. Aloufi, A. S. Alfakeeh, and F. M. Alotaibi, "An Agent-Based System for Location Privacy Protection in Location-Based Services," *ISPRS International Journal of Geo-Information,* vol. 14, no. 11, p. 433, 2025, https://doi.org/10.3390/ijgi14110433.

[23] M. Adnan, M. H. Syed, A. Anjum, and S. Rehman, "A Framework for privacy-preserving in IoV using Federated Learning with Differential Privacy," *IEEE Access,* vol. 13, pp. 13507-13521, 2025, https://doi.org/10.1109/ACCESS.2025.3526934.

[24] A. S. Alyousef, K. Srinivasan, M. S. Alrahhal, M. Alshammari, and M. Al-Akhras, "Preserving location privacy in the IoT against advanced attacks using deep learning," *International Journal of Advanced Computer Science and Applications,* vol. 13, no. 1, 2022, https://doi.org/10.14569/IJACSA.2022.0130152.

[25] L. May Petry, C. Leite Da Silva, A. Esuli, C. Renso, and V. Bogorny, "MARC: a robust method for multiple-aspect trajectory classification via space, time, and semantic embeddings," *International Journal of Geographical Information Science,* vol. 34, no. 7, pp. 1428-1450, 2020, https://doi.org/10.1080/13658816.2019.1707835.

[26] S. S. Ganorkar, S. U. Vishwakarma, and S. D. Pande, "An information security scheme for cloud based environment using 3DES encryption algorithm," *International Journal of Recent Development in Engineering and Technology,* vol. 2, no. 4, 2014.

[27] J. Li, Y. Si, T. Xu, and S. Jiang, "Deep convolutional neural network based ECG classification system using information fusion and one-hot encoding techniques," *Mathematical problems in engineering,* vol. 2018, no. 1, p. 7354081, 2018, https://doi.org/10.1155/2018/7354081.

[28] F. Alrasheedi, X. Zhong, and P.-C. Huang, "Padding module: Learning the padding in deep neural networks," *IEEE Access,* vol. 11, pp. 7348-7357, 2023, https://doi.org/10.1109/ACCESS.2023.3238315.

[29] M. S. Alrahhal, M. A. Mezher, O. A. Ghaleb, M. Al-Hjouj, R. Sehly, and S. Bataineh, "An Augmentation-Based System for Diagnosing COVID-19 Using Deep Learning," *International Journal of Advanced Computer Science & Applications,* vol. 16, no. 8, 2025, https://doi.org/10.14569/IJACSA.2025.0160819.

[30] Z. Bami, A. Behnampour, A. Bora, and H. Doosti, "A New Flexible Train-Test Split Algorithm, an approach for choosing among the Hold-out, K-fold cross-validation, and Hold-out iteration," *arXiv preprint arXiv:2501.06492,* 2025, https://doi.org/10.48550/arXiv.2501.06492.