FLOT : Location Privacy preservation in Internet of Things

Nishtha Kesswani
Central University of Rajasthan, Ajmer, India 305801
E-mail: nishtha@curaj.ac.in

Abstract. Internet of Things includes sensor enabled devices that are capable of doing a wide variety of tasks. As these devices capture huge amounts of information including the location of the user, these generate privacy concerns. In this paper, Fuzzy Logic Based Location Obfuscation Technique (FLOT), fuzzy logic based Location privacy preservation technique has been proposed. The technique was compared to other existing technique and the results indicate that the original location of the user is obfuscated to a great extent in the proposed technique.

1. Introduction
With the connected world and technologies provisioning the connections, sensor enabled Internet of Things (IoT) devices have revolutionized the world. IoT is a system of interconnected sensor enabled devices with unique identifiers and are capable of transferring data without human intervention. These devices are used in varied applications such as automation, smart cities, smart grids etc.

Augmenting the user experience with sensors and actuators enhances the capabilities of the devices, but at the same time, the devices are collecting huge amounts of data about the user. This data includes the personal details such as the date of birth of the user, her telephone number, and email address etc. which raises privacy concerns. Location-based services also collect users’ location which may be used by third party applications. Fundamental characteristics of IoT devices that make it difficult to ensure privacy are heterogeneity, inter-connectivity, dynamic networks and enormous scale. Ensuring privacy is vital not only for the safety of the users, but also to avoid intrusive interference in the personal space. In such a scenario, ensuring privacy of the users’ data and location is of utmost importance.

In this paper, a Fuzzy Logic based privacy preservation technique has been suggested. The main contribution of this piece of work is to ensure Location privacy using Fuzzy logic based obfuscation technique. The rest of the paper is organized as follows. Section 2 discusses the Background; Related Work is mentioned in Section 3. Section 4 contains the proposed Fuzzy Logic based Obfuscation Technique (FLOT). Experiments and results are given in Section 5. Section 6 concludes the paper.

2. Background
Ensuring privacy is important from the point of view of the user. There are several devices in an IoT based network that are connected to the Internet and these devices need to be protected. For instance, the user may wish to anonymize her identity, location or restrict access to her
data from third party services. In order to facilitate this, there are several different techniques that are used for privacy preservation. These include Obfuscation based techniques, Noise based techniques, and Anonymization based techniques. Figure 1 shows broad categorization of privacy preservation techniques and methods.

![Privacy preservation techniques and methods](image)

**Figure 1.** Privacy preservation techniques and methods

3. Related Work
Due to its importance, many researchers at different points of time tried to find methods of preserving privacy. For this piece of work, only Location privacy preserving techniques have been mentioned. Major works in this field are listed in Table 1.

Though there are several techniques available in literature, but most of the techniques are not suitable for the resource constrained IoT devices. An ideal privacy preservation technique should be able to ensure privacy and at the same time should be simple to implement. The technique proposed in this paper, tries to fill this research gap.
| Reference               | Privacy Preservation technique | Domain                     | Details                                                                 |
|------------------------|--------------------------------|----------------------------|------------------------------------------------------------------------|
| Beresford and Stajano[1]| Anonymization                  | Pervasive computing        | Used mix zones to ensure privacy                                       |
| Campbell et al. [3]     | Anonymization                  | Pervasive computing        | Communication infrastructure Mist that separates location from identity |
| Duckham et al.[4]       | Obfuscation                    | Context aware system       | Formal method based location obfuscation                                |
| Yingjie et al.[5]       | Anonymization                  | Mobile crowd sourcing systems | Two-stage auction algorithm based on trust degree and privacy sensibility |
| Xi et al. [6]           | Anonymization                  | Mobile online social networks | Centralized privacy preserving location sharing system                  |
| Agostino et al.[2]      | Obfuscation                    | Cellular networks          | Obfuscate the location of the user by increasing the radius, shifting the center and reducing the radius of the circle. |
| Han[7]                  | Obfuscation                    | IoT                        | Confused arc based location obfuscation                                |
| Han[8]                  | Obfuscation                    | IoT                        | k-means based approach                                                 |
| Gope et al.[9]          | Obfuscation                    | IoT                        | Privacy preserving RFID authentication scheme                            |
| Riahi et al.[10]        | Anonymization                  | IoT based transportation systems | Game theory based approach                                             |
| Jain and Kesswani [16]  | Obfuscation                    | IoT                        | Random variance added for privacy preservation                          |
| Kaur et al. [17]        | Randomization                  | IoT                        | Random path and random neighbor used for preserving location privacy     |
| Minghui et al.[11]      | Anonymization                  | Healthcare IoT             | Reinforcement learning based Privacy aware offloading with energy harvesting |
| Guan et al.[12]         | Anonymization                  | Fog enhanced IoT           | Privacy preserving data aggregation                                      |
| Jain et al.[15]         | Data splitting and obfuscation | IoT                        | Used Storage as a Service and Key Management as a Service               |
4. Fuzzy Logic based Obfuscation technique (FLOT)

4.1. System Model

Privacy preservation can be done in three ways:

- Avoiding privacy leakage by adopting the best practices that preserve privacy.
- Preventing privacy leakage by protecting points that may cause privacy leakage in the network.
- Recovery after the privacy is breached.

One such technique of preventing privacy leakage is to restrict access and reducing the points which are open to the outside network. But restricting access may not be feasible in the modern days’ connected world where all the devices are connected to each other and to the Internet.

In this paper, a Fuzzy logic based obfuscation technique has been proposed to prevent privacy leakage in IoT based networks. Let us assume the scenario given in Figure 1 in which IoT nodes are deployed. For the current piece of work, it has been assumed that the nodes are deployed randomly. In such a scenario let us assume that the attacker tries to detect the location of the user from the mobile phone shown in Figure 2. The system model consists of three components:

- IoT Network that comprises of several kinds of connected sensor enabled devices.
- User, who decides the level of privacy that she wants.
- Fuzzy Inference system that utilizes Fuzzy rules to obfuscate the location.

![System model for FLOT](image)

**Figure 2.** System model for FLOT

4.2. Adversary Model

The proposed system has three main entities; IoT devices, users and Fuzzy Inference system. The Fuzzy inference system is assumed to be a trusted entity that has complete information about the user but does not affect the privacy of the user. The attack model is as follows:

(i) Other devices in the IoT network may try to capture private information about the user.

(ii) Third parties and Location based services may use users’ location to increase user experience, but at the same time raise privacy concerns.

(iii) An intruder may enter the system and try to get users’ location and make inferences.
4.3. System Design

The location of the user is stored in a fuzzy set $A = \sum_{x \in X} (\mu_A(x))/x$ Where X is the Universe of all the locations used for the purpose of developing the system. And the membership of x in Fuzzy set A is denoted by $\mu_A(x)$. The strategy is to create 10 locations in the same fuzzy set with membership value in the range [0-1]. As the distance increases the membership value would be governed by the Gaussian membership function given in Equation 1.

$$Gaussian(x; c, \sigma) = e^{-1/2 \left( \frac{x - c}{\sigma} \right)^2}$$

For instance, let us assume that the user having the Mobile phone shown in the Figure 2 wants to obfuscate her location, and then at this particular location her membership would be defined by Equation 1. As we move away from the location of the user, the membership value would decrease. The user can obfuscate the location using 3 levels: Level 1 indicating low level of privacy, Level 2 indicating medium privacy and Level 3 indicating high level of privacy. More the level of privacy, difficult it is to get the location of the user. The Algorithm 1 and 2 for FLOT show the calculation of the obfuscated location, given the Original Location of the user. The procedure uses every 10 nearby locations and places them in the same fuzzy set whose membership is governed by Gaussian membership function mentioned in Equation 1. Larger the set, difficult it is to make inferences about the location of the user. The summary of Notations used in the Algorithm are given in Table 2.

The user is supposed to give her Privacy preference from 0 to 2. This level decides the calculation of the final obfuscated location. As indicated in the procedure, the k-nearest sets are taken into consideration with k taken from the domain (3, 5, 7) which is just indicative of increasing distance. That is, as the value of k increases, the distance between the Original Location (Loc in the Algorithm) and the Obfuscated Location (Obf) increases. The final obfuscated location is a Random point of the third, fifth and seventh set of locations. Random point is taken for the sake of convenience so that it is difficult to detect the obfuscated location.

| Term     | Description                                      |
|----------|--------------------------------------------------|
| Loc      | Original location of the user                    |
| Obf      | Obfuscated Location                              |
| LocMF    | Membership value at Original location i          |
| ObfMF    | Membership value at Obfuscated location          |
| LocFS    | Set of all Fuzzy sets of all locations           |

In Algorithm 2, Original location is in fuzzy set A and level indicates the privacy levels in fuzzy set B where $x \in A$. The obfuscated location is calculated in Algorithm 2 using Mamdani Fuzzy Inference System. The Original location and the Privacy Preference Level act as inputs and the output is final Obfuscated location. Since Mamdani Fuzzy Inference system returns a fuzzy set as output, final precise Obfuscated location is decided using Centroid de-fuzzification. Fuzzy rules used in the inference system are shown in Algorithm 2.

5. Experiments and results

The Experiments were conducted on Shared Cars Location Dataset [13]. The Dataset has five columns; Timestamp, Latitude, Longitude, TotalCars and CarsList. A snapshot of the dataset is shown in Table 3. It was pre-processed and only the relevant fields i.e. Latitude and Longitude were taken into consideration. The dataset containing 1090 records was taken for this piece of
Algorithm 1 Fuzzy Logic based Location Obfuscation Technique FLOT

Input: Original Location Loc

Output: Obfuscated Location Obf

1: ObfuscateLoc() = Function to obfuscate the Location

2: \( \text{Loc}_{MF} \leftarrow \text{Gaussian}(x; c, \sigma) = e^{(-1/2)(x-c)^2} \)

3: Levelprivacy \( \leftarrow (0, 1, 2) \) //Privacy Level selected by the user 0:Low, 1:Medium, 2: High

4: \( k \leftarrow (3, 5, 7) \) //k-Nearest Fuzzy set

5: For each fuzzyset in LocFS

6: For each Loc to be obfuscated

7: if Levelprivacy = 0 then Move to a Random point of the k nearest set then

8: Obf = ObfuscateLoc()

9: else if Levelprivacy = 1 then Move to a Random point of the k+1 nearest set then

10: Obf = ObfuscateLoc()

11: else if Levelprivacy = 2 then Move to a Random point of the k+2 nearest set then

12: Obf = ObfuscateLoc()

13: end if

14: End For

15: End For

16: Return Obf

Algorithm 2 Procedure ObfuscateLoc() for Obfuscation using Mamdani Fuzzy Inference system

FuzzyRules:

If \( x \) in original location A and level in B then obfuscated location in A + 3

If \( x \) in original location A and level in B then obfuscated location in A + 5

If \( x \) in original location A and level in B then obfuscated location in A + 7

1: Loc \( \leftarrow \) Original location of the user

2: Obf \( \leftarrow \) Obfuscated Location

3: Levelprivacy \( \leftarrow (0, 1, 2) \) //Privacy Level selected by the user 0:Low, 1:Medium, 2: High

4: \( k \leftarrow (3, 5, 7) \) //k Nearest Fuzzy set

5: For each set in k do

6: if Levelprivacy = 0 then

7: Obf \( \leftarrow \) Random(\( k \))

8: else if Levelprivacy = 1 then

9: Obf \( \leftarrow \) Random(\( k + 1 \))

10: else

11: Obf \( \leftarrow \) Random(\( k + 2 \))

12: end if

13: End For

14: Return Obf

work. Every 10 successive coordinates from the dataset were taken into one fuzzy set. Euclidean distance from the Median value was calculated using Equation 2.

\[
\sqrt{(x_1 - \text{median})^2 + (x_2 - \text{median})^2 + \ldots + (x_n - \text{median})^2}
\]  \hspace{1cm} (2)

Snapshot of the intermediate results is shown in Table 4. As seen from the results that most of the Co-ordinate locations are near the crossover points with membership value around 0.5. This is because the dataset contains co-ordinates from the same city and the locations are nearby. This problem can be solved by increasing the size of the fuzzy set to lets say 100 coordinates to
incorporate more variability and increasing the distance between the Original and Obfuscated location. Since the Obfuscated location is randomly chosen from the third, fifth and seventh consecutive sets, larger the sets are, more is the distance between the Original and obfuscated location. Thus, by regulating these parameters, the privacy level can also be regulated.

The results show that there is variation in the Original location and Obfuscated location. Table 5 shows the Original location and the location after obfuscation. The results were also compared to ESOT [14]. For instance for the same location, 51.50477 -0.1155168 (Sutton Wall, London, UK) used in ESOT gives the Obfuscated Location at 51.502966 -0.117233253 (Chicheley St. London, UK), the proposed technique FLOT gives the Obfuscated location as33.39826 4.13252 (Bou Ikerkourene, Morocco). As seen from the results that in the proposed technique FLOT, more obfuscation is achieved by increasing the distance between the Original and obfuscated location. Both the algorithms were compared on the basis of Entropy which is a measure of unpredictability. For all the location data points $d_i$ in the entire set of Locations $D$, Entropy ($E$) is measured as shown in Equation 3.

$$E = \sum_{i} \frac{d_i}{D} \log_2 \frac{d_i}{D}$$

The results indicate that the proposed approach has more unpredictability as compared to the existing approach. As the level of privacy increases, the Entropy of FLOT increases.

6. Conclusion
Ensuring location privacy is an important aspect in the modern days’ connected world. In this paper, a Fuzzy Logic based Location Obfuscation Technique was proposed and the results

| Timestamp          | Latitude  | Longitude | Totalcars | Carlist |
|--------------------|-----------|-----------|-----------|---------|
| 2019-01-10 11:45:55.070781 UTC | 32.09995  | 34.78794  | 1         | [182]   |
| 2019-01-10 11:45:55.070781 UTC | 32.06567  | 34.79612  | 1         | [268]   |
| 2019-01-10 11:45:55.070781 UTC | 32.06465  | 34.80322  | 1         | [106]   |
| 2019-01-10 11:45:55.070781 UTC | 32.05978  | 34.81034  | 1         | [180]   |
| 2019-01-10 11:45:55.070781 UTC | 32.05133  | 34.75089  | 1         | [16]    |
| 2019-01-10 11:45:55.070781 UTC | 32.04223  | 34.7742   | 1         | [72]    |
| 2019-01-10 11:45:55.070781 UTC | 32.04156  | 34.77128  | 1         | [160]   |
| 2019-01-10 11:45:55.070781 UTC | 32.12373  | 34.81346  | 1         | [210]   |
| 2019-01-10 11:45:55.070781 UTC | 32.11874  | 34.83406  | 1         | [136]   |
| 2019-01-10 11:45:55.070781 UTC | 32.03351  | 34.75509  | 1         | [27]    |
| 2019-01-10 11:45:55.070781 UTC | 32.14288  | 34.79361  | 1         | [75]    |
| 2019-01-10 11:45:55.070781 UTC | 32.14306  | 34.79729  | 1         | [132]   |
| 2019-01-10 11:45:55.070781 UTC | 32.083175 | 34.776552 | 0         | []      |
| 2019-01-10 11:45:55.070781 UTC | 32.088379 | 34.775111 | 0         | []      |
| 2019-01-10 11:45:55.070781 UTC | 32.074877 | 34.773515 | 0         | []      |
| 2019-01-10 11:45:55.070781 UTC | 32.098603 | 34.778565 | 0         | []      |
| 2019-01-10 11:45:55.070781 UTC | 32.09478  | 34.79728  | 0         | []      |
| 2019-01-10 11:45:55.070781 UTC | 32.098032 | 34.798089 | 0         | []      |
| 2019-01-10 11:45:55.070781 UTC | 32.12047  | 34.800318 | 0         | []      |
| 2019-01-10 11:45:55.070781 UTC | 32.04409  | 34.80421  | 0         | []      |
Table 4. Snapshot of the Intermediate results

| Latitude  | Longitude  | X1-Median | X2-median | Euclidean Distance | Membership |
|-----------|------------|-----------|-----------|--------------------|------------|
| 32.03025  | 34.74837   | 1.3614    | 1.35672   | 1.922003933        | 0.52090298 |
| 32.03025  | 34.74837   | 1.3614    | 1.35672   | 1.922003933        | 0.52090298 |
| 32.03028  | 34.74837   | 1.36137   | 1.35672   | 1.921982683        | 0.52090051 |
| 32.03049  | 34.74791   | 1.36116   | 1.35626   | 1.921509233        | 0.52042424 |
| 32.03551  | 34.75509   | 1.35814   | 1.36344   | 1.924451323        | 0.51962862 |
| 32.035393 | 34.75873   | 1.356257  | 1.356708  | 1.925705267        | 0.51929026 |
| 32.035393 | 34.75873   | 1.356257  | 1.356708  | 1.925705267        | 0.51929026 |
| 32.035393 | 34.75873   | 1.356257  | 1.356708  | 1.925705267        | 0.51929026 |
| 32.035393 | 34.75873   | 1.356257  | 1.356708  | 1.925705267        | 0.51929026 |
| 32.035393 | 34.75873   | 1.356257  | 1.356708  | 1.925705267        | 0.51929026 |
| 32.035393 | 34.75873   | 1.356257  | 1.356708  | 1.925705267        | 0.51929026 |
| 32.035393 | 34.75873   | 1.356257  | 1.356708  | 1.925705267        | 0.51929026 |
| 32.035393 | 34.75873   | 1.356257  | 1.356708  | 1.925705267        | 0.51929026 |

Table 5. Experimental results after applying FLOT

| Original location | Original location coordinates | Obfuscated location | Obfuscated location coordinates | Privacy Level | Distance (kms) |
|-------------------|-------------------------------|--------------------|---------------------------------|---------------|----------------|
| Bat Yam, Israel   | 32.03025 34.74837             | Gunbad, Pakistan   | 33.39165 68.93284               | 2             | 3247           |
| Aviv Yado, Israel | 32.041052 34.769815           | Haven Park, Western Australia | 33.40569 117.22228             | 3             | 11100          |
| Middleburg, Netherlands | 51.50477 -0.1155168 | Bou Ikerkourene, Morocco | 33.39826 4.13252               | 1             | 2106           |

indicate that the Original location of the user is obfuscated to a great extent. In the proposed technique FLOT, as the Level of obfuscation increases, the location privacy increases. The advantage of the proposed technique is its simplicity.

References
[1] Beresford, Alastair R., and Frank Stajano. "Mix zones: User privacy in location-aware services." IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second. IEEE, 2004.
[2] Ardagna, Claudio Agostino, et al. "Location privacy protection through obfuscation-based techniques." IFIP Annual Conference on Data and Applications Security and Privacy. Springer, Berlin, Heidelberg, 2007.
[3] Campbell, Roy, et al. "Towards security and privacy for pervasive computing." International Symposium on Software Security. Springer, Berlin, Heidelberg, 2002.
[4] Duckham, Matt, and Lars Kulik. "A formal model of obfuscation and negotiation for location privacy." International conference on pervasive computing. Springer, Berlin, Heidelberg, 2005.

[5] Wang, Yingjie, et al. "Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems." Computer Networks 135 (2018): 32-43.

[6] Xiao, Xi, et al. "CenLocShare: a centralized privacy-preserving location-sharing system for mobile online social networks." Future Generation Computer Systems 86 (2018): 863-872.

[7] Han, Guangjie, et al. "CASLP: A confused arc-based source location privacy protection scheme in WSNs for IoT." IEEE Communications Magazine 56.9 (2018): 42-47.

[8] Han, Guangjie, et al. "KCLP: A k-means cluster-based location privacy protection scheme in WSNs for IoT." IEEE Wireless Communications 25.6 (2018): 84-90.

[9] Gope, Prosanta, et al. "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment." Future Generation Computer Systems 83 (2018): 629-637.

[10] Sfar, Arbia Riahi, et al. "A Game Theoretic Approach for Privacy Preserving Model in IoT-Based Transportation." IEEE Transactions on Intelligent Transportation Systems (2019).

[11] Min, Minghui, et al. "Learning-based privacy-aware offloading for healthcare IoT with energy harvesting." IEEE Internet of Things Journal (2018).

[12] Guan, Zhitao, et al. "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT." Journal of Network and Computer Applications 125 (2018): 82-92.

[13] Shared Cars location, Kaggle, Available: https://www.kaggle.com/doit-intl/autotel-shared-car-locations/version/1?

[14] Ullah, Ikram, et al. "ESOT: A new privacy model for preserving location privacy in Internet of Things." Telecommunication Systems 67.4 (2018): 553-575.

[15] Jain, Shelendra Kumar, Nishtha Kesswani, and Basant Agarwal. "Security, privacy and trust: privacy preserving model for internet of things." International Journal of Intelligent Information and Database Systems 13.2-4 (2020): 249-277.

[16] Jain, Shelendra Kumar, and Nishtha Kesswani. "IoTP an Efficient Privacy Preserving Scheme for Internet of Things Environment." International Journal of Information Security and Privacy (IJISP) 14.2 (2020): 116-142.

[17] Kaur, Rajwinder, et al. "Efficient Routing Protocol for Location Privacy Preserving in Internet of Things." International Journal of Information Security and Privacy (IJISP) 13.1 (2019): 70-85.