Location-Aware Privacy Preserving Scheme in SDN-Enabled Fog Computing

Bruce Gu[1], Xiaodong Wang[1], Youyang Qu[1], Jiong Jin[2], Yong Xiang[1], and Longxiang Gao[1(✉)]

[1] Deakin University, 221 Burwood Highway, Burwood, VIC, Australia
{bgu,xdwang,y.qu,yong.xiang}@deakin.edu.au
[2] Swinburne University of Technology, John Street, Hawthorn, VIC, Australia
jiongjin@swin.edu.au

Abstract. Fog computing, as a novel computing paradigm, aims at alleviating data loads of cloud computing and brings computing resources closer to end users. This is achieved through fog nodes such as access points, sensors, and fog servers. According to the fog computing location awareness capabilities, a large quantity of devices exists in the physical environment with a short cover range. This leads to location privacy exposure by the connection triggered. Adversaries can pry into more private data through the commodiously accessible location information. Although the existing privacy-preserving schemes can address some issues such as differential privacy, it cannot meet various privacy expectations in practice for fog computing variants. Motivated by this, we propose a location-aware dynamic dual ϵ-differential privacy preservation scheme to provide the ultimate protection. We start by establishing the first scheme by clustering fog nodes with SDN-enabled fog computing. In addition, we customize ϵ-differential privacy preservation scheme to tailor-made for the variant fog computing services. Furthermore, we employ a modified Laplacian mechanism to generate noise, with which we find the optimal trade-off. Extensive experimental results confirm the significance of the proposed model in terms of privacy protection level and data utility.

Keywords: Differential privacy · Fog computing · Software defined network

1 Introduction

With the rapid development of the fog computing [3], connectivity between fog nodes is becoming stronger and more ubiquitous. An increasing volume of entities are becoming intelligent and serving as fog nodes. They can perceive the surrounding environment, connect to the Internet, and receive commands remotely by their location information. The intelligence of these fog nodes is the result of data, analysis, and feedback from various systems or servers of different mobile devices. A large amount of the data leads to an increased possibility of privacy

S. Yu et al. (Eds.): SPDE 2020, CCIS 1268, pp. 176–190, 2020.
https://doi.org/10.1007/978-981-15-9129-7_13

issues such as location-aware privacy, sensitive context-aware privacy, etc. [7,8]. Therefore, it is necessary to protect the privacy between fog computing devices and users among the network infrastructure.

According to the fog computing reference model [4], location-based services have been widely used [24], for example, vehicular systems, smart grid, and smart city. Traditionally, end devices are required to connect to the best available fog node in order to improve user experience in a convenient way [16]. Location-aware privacy issues occur when the transmission has been confirmed [25]. Adversaries can easily detect and attack fog nodes in an appropriate manner. The main challenge for location-aware fog computing systems is how to securely and efficiently provide privacy-preserving methodologies among a large number of devices that contain sensitive location information [18].

Furthermore, with the growing demand for data, users' personal information can be disclosed against users' willing. However, with the potential threat of untrustworthy of the location service provider (fog node) and user sensitive information leakage, fog nodes containing the threat from users' privacy in the collection, distribution and use of location information [22]. Although some data privacy-preserving methods or algorithms are promoted, it is impractical for traditional privacy-preserving techniques to directly address the identified problem in an appropriate manner.

In this paper, in order to obtain an optimal tradeoff with high accuracy and efficiency, we propose a Dynamic Dual Scheme ϵ-Differential Privacy model (DDSDP) based on software-defined fog computing services. Software-defined fog computing provides the network with programmability and privacy protection in a flexible and dynamic way. In the proposed model, we use dual schemes to obtain tradeoff optimization. Firstly, we start from the fog nodes clustering approach. This approach brings the user into fog computing services by connecting with a group of fog nodes instead of one stable service provider, while it increases the difficulty when adversaries approach their collision attack. We customize ϵ-differential privacy based on the distance between clustered fog nodes. Moreover, we develop a QoS-based mapping function to measure data utilities and privacy protection level. Our extensive experiments indicate the efficiency and accuracy in a dynamic manner.

The main contributions of this work are summarized as follows.

- We propose a Dynamic Dual ϵ-Differential Privacy scheme (DDSDP) to preserve location-aware privacy. We consider a dynamic clustered connection for the fog nodes in the initial stage. This preserved direct attack from adaptable adversaries. According to customized Laplacian Mechanism differential privacy preservation setup, we customized protection levels and data utilities in order to achieve optimal protection.
- We analyze and modify the SDN-based fog computing control layer known as Dynamic Solution Layer (DSL). It dynamically customizing the clustering level to respond to different clustering situations. It protects from a stabilized system to a random variable system. Moreover, it increases the difficulty level for adversaries to analyze the real location of the user.

– We conduct experiments on a real-world dataset to demonstrate the proposed algorithms. The evaluation results show the significant performances in terms of data utility and privacy protection level regarding location-aware applications, respectively.

The remaining part of this paper is organized as follows. Section 2 introduces the related work and a literature review from the existing problems and solutions. We prompt the dynamic solution layer from modified SDN-based fog computing in Sect. 3. Followed by system modelling and analysis in Sect. 3. The system performance and evaluation are described in Sect. 4. Finally, we summarized and conclude this paper in Sect. 6.

2 Related Work

Fog computing brings data closer to the user instead of relying on communication with the data center [6]. One of the key benefits of fog computing is the dense geographical distribution that can be achieved by deploying fog nodes in different locations and connecting each of these nodes to end devices [20]. This geographical distribution enables more efficient communication between end users or devices and the server. The geographical distribution of the fog nodes also enables location-based mobility support for IoT devices such that traversal of the entire network is not necessary [22]. This is distinct from the situation in a cloud network, in which all data must be uploaded to the cloud side for computation and data packets must then be sent back to the end devices [12]. This delays the communication of data, especially in environments with real-time application requirements such as for the control of oil pump valves. Apart from all the beneficial location-aware features from fog computing, the leading problem appears. The protection of users' location privacy heave in sight.

According to the location-aware privacy preserving issues in fog computing, a few papers considered problem [14,22]. Approaches including k-anonymity based privacy preservation, t-Closeness and other variants. In addition, privacy-preserved pseudonym scheme proposed by J. Kang [10] has been discussed privacy issues in location based fog computing Internet vehicles. Qu et al. proposed a GAN-driven location privacy-preserving method by means of differential privacy [17,19]. Although these technologies provided well-performance results, they are more focusing on a stabilized network condition instead of dynamic and customized fog computing constrains.

SDN has been proved and widely applied on fog computing infrastructure [9, 11]. SDN is designed to solve the challenges within fog computing by decoupling data and control plane. The integration between SDN and fog computing can effectively improve the performance of the IoTs. Although the deployment of SDN with fog computing seems promising, the privacy issues can not be avoided [2].

Lyu [13] conducted deep research on the customized ϵ-differential privacy preserving methodology and successfully proven by Qu [15], Badsha [1] and Wang

[23]. These approaches have high effectiveness in social network, recommender system, and location-aware applications. They have solid theoretical foundations as well as providing high level privacy protections [21].

3 System Modelling and Analyze

In this section, we present our dynamic dual ϵ-differential privacy preserving (DDSP) scheme in SDN enabled fog computing service. This dynamic model focus on protecting location-aware privacy content occurred between users and fog nodes. We first introduce a modified control layer from SDN infrastructure, named as Dynamic Solution Layer (DSL). This new control layer aims to provide a dynamic clustering solution rely on the reality transmission. Each cluster creation is based on modified Affinity Propagation (AP) clustering method. In this approach, adversaries are not be able to determine the source of the initial connected fog node as the clusters are dynamically updated. Therefore, this clustering approach create fist privacy protection. Moreover, we present modified Laplacian Mechanism and add Laplacian Noise to increase the protection level. We use QoS mapping method to measure the distance between each cluster. Thus, the ultimate dual protection of the privacy in terms of privacy level and data utility has been created in SDN enable fog computing services.

3.1 Dynamic Solution Layer

In this section, we present the proposed innovative architecture that integrates the fog computing environment with SDN. As shown in Fig. 1, two main physical device component layers are proposed in our architecture: the control layer and the infrastructure layer.

In our proposed reference model, programmability is proposed to analyze the location information and user data to determine the quantity of fog nodes involved. Furthermore, in the clustering condition, two or more fog nodes are assigned to perform location aware analyze as well as providing fuzzification towards adversaries attack. Clustering method is a virtualized network based on geographically distributed fog nodes. In reality, all fog nodes are still physically located at their original locations, but nm virtually, they are clustered via SDN to improve their location fuzzification. For example, adversary aims to attack a user. In traditional methodology, user connect with the closest or best signal fog node. However, adversary will easily determine the exact location. Instead, when user first create transmission with fog computing network, they connect to the clustered fog nodes which contains two or more available. Adversary only be able to determine the clustered fog nodes instead of locating the exact fog node to obtain the true location information.

DSL also provide a dynamic feedback solution for end users to improve the protection level of privacy. All clustering updates and reunited with different fog nodes operate in this layer. In other word, the cluster for our proposed model is dynamic. Reunited and updates will be defined when connection capacity reach

limitation. Each fog nodes has theoretic limitation, DSL also be responsible for QoS data utility measurement.

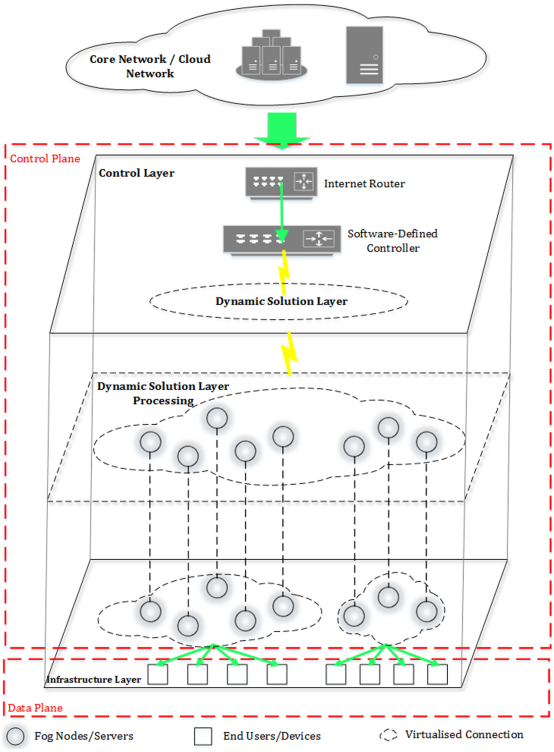

Fig. 1. Overview of the dynamic solution layer within SDN based fog computing.

3.2 Virtualized Fog Node Clustering

Virtualized clustering is our first scheme in terms of privacy preserving in our proposed model. First of all, we formulate the fog node location of Fog Computing as a clustering problem with multi constraints. The vitalization for the clustering organiszed by SDN controller demonstrates in Fig. 2.

Entropy Weight Method Based Cluster Triggering. The basic idea of the EWM is to determine objective weights based on the variability of certain indicators. In our scenario, the EWM is applied to calculate the weight of each element in each dimension. Generally, a smaller elemental entropy e^j indicates that an element is more meaningful, providing more information and related to more data in the fog network environment, and thus should be assigned a greater weight in the associated dimension. On the other hand, a larger entropy e^j indicates that an

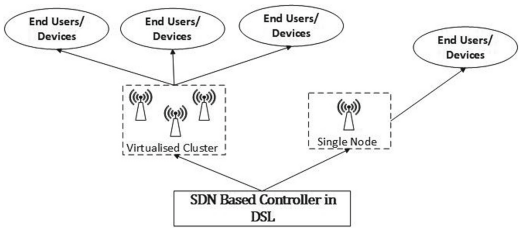

Fig. 2. Vitualized fog clustering by SDN controller.

element is of smaller value, provides less information, and plays a smaller role in the overall evaluation, and thus, it should have a smaller weight.

Unification Process and Weight Factors. For the overall network environment, the SDN controller collects and stores all fog node location identification numbers and specifications. Based on the historical data collected ahead of time, the SDN controller places all elements and factors into a matrix F, where the elements $F = F_1^1, F_2^1, F_3^1, F_\beta^1$ represent different factors of the same fog node and the elements $F = F_1^1, F_1^2, F_1^3, F_1^\alpha$ represent the same factor for different fog nodes.

$$F = \begin{bmatrix} F_1^1 & F_2^1 & F_3^1 & \dots & F_\beta^1 \\ F_1^2 & F_2^2 & F_3^2 & \dots & F_\beta^2 \\ & & \cdots\cdots & & \\ F_1^\alpha & F_2^\alpha & F_3^\alpha & \dots & F_\beta^\alpha \end{bmatrix} \tag{1}$$

Since all factors have different indices, a unification process is required before the aggregate indicator can be calculated. More specifically, the absolute values must be converted to relative values to solve the problem of different absolute values for different indices. The matrix F after the unification process is denoted by F'.

$$F' = \begin{bmatrix} \frac{F_1^1}{\sum_{i=1}^{\alpha} F_1^i} & \frac{F_2^1}{\sum_{i=1}^{\alpha} F_2^i} & \frac{F_3^1}{\sum_{i=1}^{\alpha} F_3^i} & \cdots & \frac{F_\beta^1}{\sum_{i=1}^{\alpha} F_\beta^i} \\ \frac{F_1^2}{\sum_{i=1}^{\alpha} F_1^i} & \frac{F_2^2}{\sum_{i=1}^{\alpha} F_2^i} & \frac{F_3^2}{\sum_{i=1}^{\alpha} F_3^i} & \cdots & \frac{F_\beta^2}{\sum_{i=1}^{\alpha} F_\beta^i} \\ & & \cdots\cdots\cdots\cdots & & \\ \frac{F_1^\alpha}{\sum_{i=1}^{\alpha} F_1^i} & \frac{F_2^\alpha}{\sum_{i=1}^{\alpha} F_2^i} & \frac{F_3^\alpha}{\sum_{i=1}^{\alpha} F_3^i} & \cdots & \frac{F_\beta^\alpha}{\sum_{i=1}^{\alpha} F_\beta^i} \end{bmatrix} \tag{2}$$

Since the unification process has been applied, the weight factor must be calculated for each factor j in each dimension i, where $i = 1, 2, ..., n$ and $j = 1, 2, ..., m$.

$$p_{ij} = \frac{F'_{ij}}{\sum_{i=1}^{n} x_{ij}} \tag{3}$$

Once the weight factors have been calculated, the entropy value of each factor j must be calculated, where $j = 1, 2, ..., m$. Here, $k = 1/\ln(n) > 0$ and $e_j >= 0$.

$$e_j = -k \sum_{i=1}^{n} p_{ij} \ln p_{ij} \tag{4}$$

A redundancy rate is calculated to reduce the deviation during this process. For $j = 1, 2, ..., m$, the redundancy rate will be $d_j = 1 - e_j$. The weight factors after the redundancy correction are calculated as follows:

$$w_j = \frac{d_j}{\sum_{j=1}^{m} d_j} \tag{5}$$

Cluster Triggering Process. Since the weight factors for each element in each dimension have been determined, the clustering process is performed based on these weight factors. Suppose that t_{trig} is the threshold level for triggering clustering and depends on the environment of the fog network and that T_{trig} is the result of the triggering process and depends on each element and its calculated weight factor. The clustering result depends on the fog node factor that is associated with the maximum value.

$$T_{trig}^{1} = \frac{F_1^1}{\sum_{i=1}^{\alpha} F_1^i} \times t_{trig}$$

$$T_{trig}^{2} = \frac{F_2^1}{\sum_{i=1}^{\alpha} F_2^i} \times t_{trig}$$

$$\cdots$$

$$T_{trig}^{\beta} = \frac{F_\beta^1}{\sum_{i=1}^{\alpha} F_\beta^i} \times t_{trig}$$

$$T_{trig} = max(T_{trig}^{1}, T_{trig}^{2}, \ldots, T_{trig}^{\beta}) \tag{6}$$

3.3 Affinity Propagation Based Clustering

Affinity propagation (AP) is a semi-supervised clustering algorithm based on nearest neighbor propagation that was proposed by [5]. Unlike in other clustering methods, in AP, it is not necessary to specify the final number of clusters. The cluster centers are selected from among the existing location data points instead of being generated as new data points. The model of the AP clustering method is less sensitive to the initial input location data and does not require the data similarity matrix to be symmetric. In a fog network, the input data can be of different types due to the different selections made by our triggering process based on the weight factors. Therefore, the AP algorithm is most suitable for clustering the fog nodes.

Preference. The clustering center similarity, $sim(i, k)$, represents the similarity between data point i and data point k. This similarity is calculated using the Euclidean distance:

$$sim(i, k) = \sqrt{\sum_{r=1}^{n} (i - k)^2} \times T_{trig} \tag{7}$$

Responsibility. In the responsibility matrix, $r(i,k)$ denotes the extent to which data point k is suitable for being designated as the cluster center for data point i and represents a message sent from i to k, where $k \in 1, 2, ..., N$ and $k \neq k'$.

$$r(i,k) = (s(i,j) - max\left\{a(i,k') + sim(i,k')\right\}) \times T_{trig} \tag{8}$$

In the above equation, $a(i,k)$ is a value representing the availability of point i to a point other than k, and its initial value is 0. $s(i,k)$ denotes the responsibility of points other than k to point i, where points outside of i are competing for the ownership of i. $r(i,k)$ denotes the cumulative responsibility of k to become the cluster center for i. When $r(i,k) > 0$, this indicates a greater responsibility of k to become the cluster center.

Availability. The availability $a(i,k)$ denotes the likelihood that data point i will select data point k as its cluster center and represents a message sent from k to i.

$$a(i,k) = min\left\{0, r(k,k) + \sum_{k}\left\{max(0, r(i',k))\right\}\right\} \times T_{trig} \tag{9}$$

$$a(k,k) = (\sum_{k}\left\{max(0, r(i',k))\right\}) \times T_{trig} \tag{10}$$

Here, $r(i',k)$ denotes the responsibility value of point k as the cluster center for points other than i; all responsibility values that are greater than or equal to 0 are summed, and we also add the responsibility value of k as its own cluster center. Specifically, point k is supported by all data points with corresponding responsibility values greater than 0, and data point i selects k based on its cumulative value as a cluster center.

Damping Factor λ. As the algorithm iteratively updates the values of availability and responsibility, a damping factor is applied. The effect of this factor λ is to enable the AP algorithm to converge more efficiently. The damping factor takes on values between 0 and 1. During each iteration of the algorithm, λ acts on the responsibility and availability values to weight the update relative to the previous iteration.

$$r_n = (1 - \lambda) \times r_n + \lambda \times r_{n-1} \tag{11}$$

$$a_n = (1 - \lambda) \times a_n + \lambda \times a_{n-1} \tag{12}$$

3.4 Laplacian Mechanism and Laplacian Noise

We probabilistic the original single clustering query results to protect location privacy. In order to protect users' location-aware content privacy, we use Laplacian mechanism to change the real value by adding Laplacian noise to the original clustering result data, so that the differential privacy is satisfied before and after adding noise.

$$
\begin{aligned}
&M(D) = f(D) + Y \\
&\text{s.t.} \\
&Lap(\alpha) = \frac{p_x(z)}{p_y(z)} = exp(\frac{\epsilon \cdot \parallel f(x) - f(y) \parallel}{\triangle f})
\end{aligned}
\tag{13}
$$

where ϵ defines privacy budget, ϵ can be customized due to the clustering requirement in order to achieve better privacy budget result. Y determines Laplacian distributed noise. $Lap(\alpha)$ defines the probability density of the mechanism while α decides the size of the noise.

3.5 QoS Data Utility Mapping

In the DDSDP model, we have defined the distance between each cluster $sim(i,k)$ in early paragraph, we use Softmax function to model QoS data utility function and privacy protection level ϵ. The softmax function assigns decimal probabilities to each class in a multiclass problem. It is also widely used to mapping the data utility and privacy protection level according to the QoS. The mapping function illustrated as

$$
\mathrm{QoS}(\epsilon_i) = k \times \frac{\exp(\theta_i^t sim_{ik} \cdot x)}{\sum_{k=1}^{K} \exp(\theta_k^t sim_{ik} \cdot x)} \tag{14}
$$

where $k \in K$ and defined as the parameter to adjust the maximum amplitude value, θ is determined the steepness of the curve and x denotes the location.

3.6 Dynamic Dual Scheme Differential Privacy

In fog computing, each user publishes their sensitive location data upon the connection created. However, these location information needs privacy protection before been published. We have created first scheme to increase the difficulty level when adversary aims to attack. Furthermore, our second scheme aims to provide ultimate privacy protection to the users. We use ϵ-Customizable Differential Privacy to obtain our goal. We formulated the mechanism when $M \to \Delta(\chi)$ is considered to be ϵ-differentially privacy as

$$
\begin{aligned}
&Pr\left[M(D) \in \Omega\right] = \exp(QoS(\epsilon_i)) \cdot Pr\left[M(D') \in \Omega\right] \\
&= \exp(k \times \frac{\exp(\theta_i^t sim_{ik} \cdot x)}{\sum_{k=1}^{K} \exp(\theta_k^t sim_{ik} \cdot x)}) \cdot Pr\left[M(D') \in \Omega\right] \\
&\text{s.t.} \\
&\forall \Omega \subseteq \chi, \\
&\forall (D, D') \subseteq \psi,
\end{aligned}
\tag{15}
$$

where χ denotes noisy outcome and D defines the space of the sensitive location data, where $\epsilon \geq 0$, and $\psi \subseteq \forall (D, D') \subseteq \psi$ denotes proximal relation between the data.

4 Performance Evaluation

In this section, we run a series of simulations to testify the performance of our proposed DDSDP model in serval ways. First, we evaluate the data utilities by sampling time slot with different location; then, we evaluate privacy protection level with different time slot by different locations. Third part of the experiment would evaluate the performance of the clustering approach including clustering results, transmission results, clustering distance, and loading performance for the overall fog nodes. In order to verify these results, we use latest version of the "VicFreeWiFi Access Point Locations" dataset, which contains 571 raw data of location information. This dataset is available in serval locations across 300 kms and it allows 250 MB per devices, per day. Within the dataset, it contains detailed location information for the access points, including 391 nodes recorded in city center, 44 nodes in northbound area, and 82 nodes west-northbound area. These location information leads the location-aware issues for adversaries to determine the users.

In the following experiments, we compare our model with different ϵ value in order to obtain the best performance and customization of the ϵ-differential privacy protection scheme. Moreover, we also evaluate the performance of the clustering efficiency as SDN-enabled fog computing should contains more customizations features without effect original performance. Respectively, the SDN enabled clustering results demonstrates better network performance.

4.1 Data Utilities Performance

Figure 3 shows the results of the data utilities according to our DDSDP model. This figure demonstrate the general trends of the QoS functionality. We selected three customized representative parameter values for the ϵ, which when $\epsilon = 1$, $\epsilon = 0.5$, and $\epsilon = 0.1$, by comparing with raw data value to observe our results, which makes it applicable to various scenarios. We start with clustering algorithm to choose 20 available clustered fog network, these clustered network based on QoS measurement from the clustering distances. Laplacian mechanism is responsible to generate noisy responses. As shown in the figure, smaller ϵ values leads better overall data utility performance value. For the particular dataset scenarios, when ϵ value equals to 0.1, we have achieve the peak value which is 1.7 with clustering time slot 5.

4.2 Privacy Protection Level Evaluation

We consider different clustering situations in terms of the performance for privacy protection level. In the initialization stage, we enabled three representative parameter value same with data utilities evaluation to setup the customized ϵ. The reason to choose three ϵ value aim to simulate the randomness of Laplacian mechanism which leads to different noisy responses. As shown in Fig. 4, privacy protection level comparison in term of customizable ϵ is based on cluster distance. Sampling time slot 7 with one of the cluster reach the maximum privacy

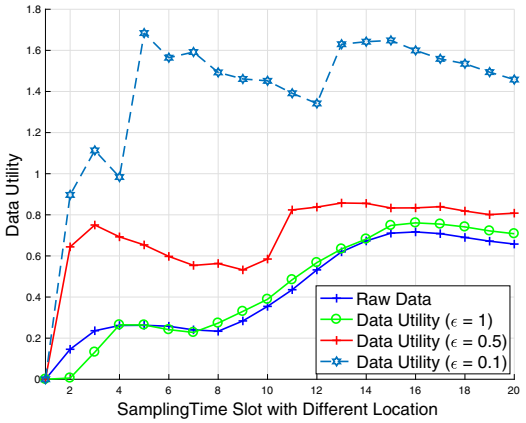

Fig. 3. Data utilities performance among three ϵ values.

protection level as 1.5, as well as the cluster in time slot 20 remain to the highest value along with other three values. Although the performance for three parameters retains different results from different cluster, it justifies the outstanding importance of the customization. For example, for time slot 4's cluster, we should select customized the ϵ value to 1, respectively.

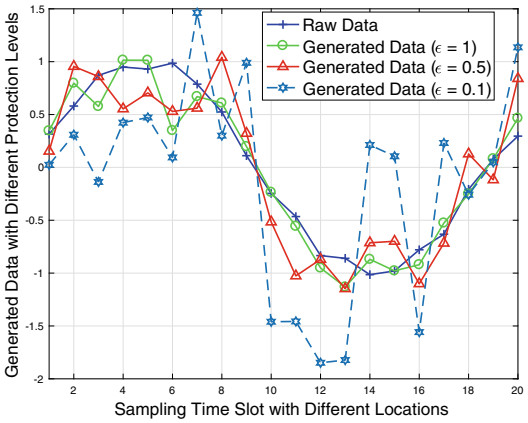

Fig. 4. Privacy levels with different locations.

4.3 Clustering Efficiency Performance

Figure 5 shows the node clustering results generated via the AP clustering method in the DSL. In these results, the estimated number of clusters is 16, and

these clusters are formed from 517 available fog nodes. We tested three similarity values to evaluate the system performance. Among the results, the minimum similarity is $2.000000e^{-8}$, and the median and maximum similarity values are 0.017874 and 1.276488, respectively. The similarity is based on the longitudinal and latitudinal locations along with the connection speed. The homogeneity rate is 0.513, which indicates the extent to which nodes with the same properties are clustered. In this particular dataset, the rate is based predominantly on the connection speed. The completeness and V-measure results are 0.133 and 0.211, respectively, and the adjusted Rand index is 0.080. The clustering results were generated by the DSL system and show good performance.

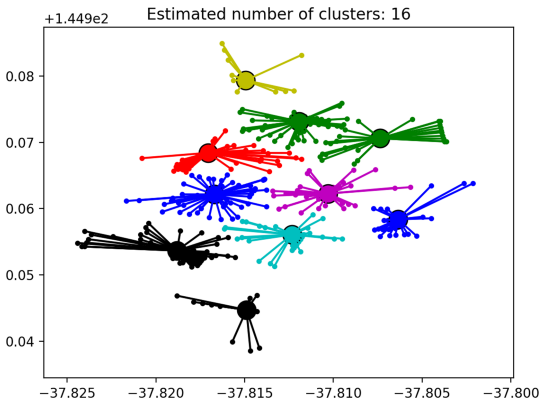

Fig. 5. Efficiently clustered results.

One of the key factors in testing the performance of the clustered network is the file transmission speed. As seen from our simulations, the standard fog network is better able to handle a small amount of data. However, as the file size grows, the performance of the resource-sharing clustered network becomes superior to that of the standard network, as shown in Fig. 6. In both simulations, the dataset was run from the same starting level of zero. As the file transmission time increases with increasing file size, the two systems perform almost the same in the range of 4000 MB to 5000 MB. However, when the file size is over 5000 MB, the speed gap becomes increasingly larger with increasing file size. This is because of the power of sharing computing capacities among the nodes, which enables the borrowing of other nodes to help with computations.

In Fig. 6, we conducted file loading times for videos downloaded from 200 different fog nodes, where the upper line is the video loading time in the clustered fog environment and the lower line is the result without clustering. Therefor, there are large time fluctuations in the non-clustered environment as the end device keeps trying to find a node that is available for downloading. By contrast, the upper line shows a significantly more stable loading time, reflecting an improved user experience.

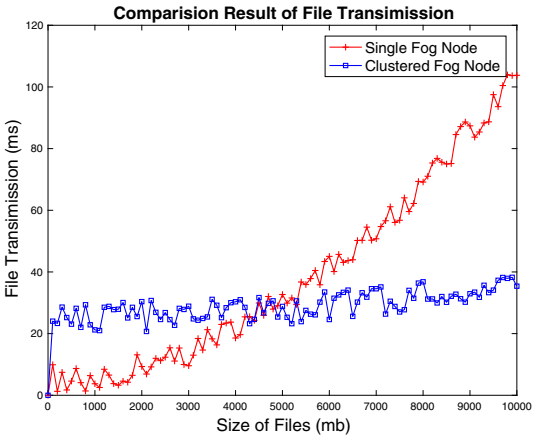

Fig. 6. Comparison of file transmission results.

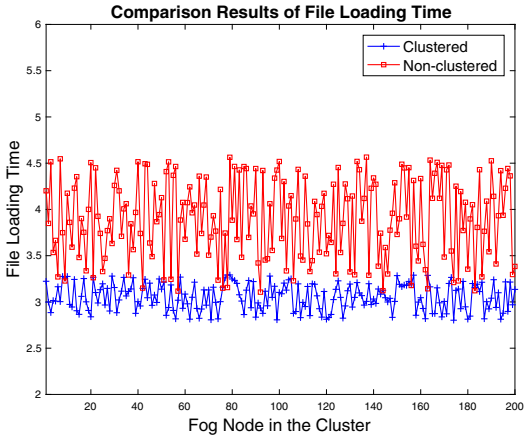

Fig. 7. Comparison of file loading time.

In conclusion, the proposed DDSDP model shows high quality dual scheme privacy protection level in terms of data utility and privacy protection level (Fig. 7).

References

1. Badsha, S., et al.: Privacy preserving location-aware personalized web service recommendations. IEEE Trans. Serv. Comput. 1 (2018). https://doi.org/10.1109/TSC.2018.2839587
2. Baktir, A.C., Ozgovde, A., Ersoy, C.: How can edge computing benefit from software-defined networking: a survey, use cases, and future directions. IEEE Commun. Surv. Tutor. **19**(4), 2359–2391 (2017). https://doi.org/10.1109/COMST.2017.2717482

3. Bonomi, F., Milito, R., Natarajan, P., Zhu, J.: Fog computing: a platform for internet of things and analytics. In: Bessis, N., Dobre, C. (eds.) Big Data and Internet of Things: A Roadmap for Smart Environments. SCI, vol. 546, pp. 169–186. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-05029-4_7
4. Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, MCC 2012, New York, NY, USA, pp. 13–16. ACM (2012). https://doi.org/10.1145/2342509.2342513. http://doi.acm.org/10.1145/2342509.2342513
5. Frey, B.J., Dueck, D.: Clustering by passing messages between data points. Science **315**(5814), 972–976 (2007). https://doi.org/10.1126/science.1136800. http://science.sciencemag.org/content/315/5814/972
6. Gao, L., Luan, T.H., Yu, S., Zhou, W., Liu, B.: FogRoute: DTN-based data dissemination model in fog computing. IEEE Internet of Things J. **4**(1), 225–235 (2017)
7. Gu, B., Wang, X., Qu, Y., Jin, J., Xiang, Y., Gao, L.: Context-aware privacy preservation in a hierarchical fog computing system. In: ICC 2019–2019 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2019)
8. Gu, B.S., Gao, L., Wang, X., Qu, Y., Jin, J., Yu, S.: Privacy on the edge: Customizable privacy-preserving context sharing in hierarchical edge computing. IEEE Trans. Netw. Sci. Eng. (2019)
9. Kadhim, A.J., Hosseini Seno, S.A.: Maximizing the utilization of fog computing in internet of vehicle using SDN. IEEE Commun. Lett. **23**(1), 140–143 (2019)
10. Kang, J., Yu, R., Huang, X., Zhang, Y.: Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. IEEE Trans. Intell. Transp. Syst. **19**(8), 2627–2637 (2018)
11. Li, C., Qin, Z., Novak, E., Li, Q.: Securing SDN infrastructure of IoT? Fog networks from MITM attacks. IEEE Internet of Things J. **4**(5), 1156–1164 (2017)
12. Luan, T.H., Gao, L., Li, Z., Xiang, Y., Sun, L.: Fog computing: focusing on mobile users at the edge. CoRR abs/1502.01815 (2015). http://arxiv.org/abs/1502.01815
13. Lyu, L., Nandakumar, K., Rubinstein, B., Jin, J., Bedo, J., Palaniswami, M.: PPFA: privacy preserving fog-enabled aggregation in smart grid. IEEE Trans. Ind. Inf. **14**(8), 3733–3744 (2018). https://doi.org/10.1109/TII.2018.2803782
14. Ma, L., Liu, X., Pei, Q., Xiang, Y.: Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing. IEEE Trans. Serv. Comput. 1 (2018). https://doi.org/10.1109/TSC.2018.2825986
15. Qu, Y., Yu, S., Gao, L., Zhou, W., Peng, S.: A hybrid privacy protection scheme in cyber-physical social networks. IEEE Trans. Comput. Soc. Syst. **5**(3), 773–784 (2018). https://doi.org/10.1109/TCSS.2018.2861775
16. Qu, Y., et al.: Decentralized privacy using blockchain-enabled federated learning in fog computing. IEEE Internet of Things J. (2020)
17. Qu, Y., Yu, S., Zhang, J., Binh, H.T.T., Gao, L., Zhou, W.: GAN-DP: generative adversarial net driven differentially privacy-preserving big data publishing. In: ICC 2019–2019 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2019)
18. Qu, Y., Yu, S., Zhou, W., Peng, S., Wang, G., Xiao, K.: Privacy of things: emerging challenges and opportunities in wireless internet of things. IEEE Wireless Commun. **25**(6), 91–97 (2018). https://doi.org/10.1109/MWC.2017.1800112
19. Qu, Y., Yu, S., Zhou, W., Tian, Y.: GAN-driven personalized spatial-temporal private data sharing in cyber-physical social systems. IEEE Trans. Netw. Sci. Eng. (2020)

20. Stojmenovic, I., Wen, S.: The fog computing paradigm: scenarios and security issues. In: 2014 Federated Conference on Computer Science and Information Systems, pp. 1–8, September 2014. https://doi.org/10.15439/2014F503
21. Wang, Q., Chen, D., Zhang, N., Ding, Z., Qin, Z.: PCP: a privacy-preserving content-based publish? Subscribe scheme with differential privacy in fog computing. IEEE Access **5**, 17962–17974 (2017). https://doi.org/10.1109/ACCESS.2017.2748956
22. Wang, T., Zhou, J., Chen, X., Wang, G., Liu, A., Liu, Y.: A three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing. IEEE Trans. Emerg. Topics Comput. Intell. **2**(1), 3–12 (2018). https://doi.org/10.1109/TETCI.2017.2764109
23. Wang, W., Zhang, Q.: Privacy preservation for context sensing on smartphone. IEEE/ACM Trans. Netw. **24**(6), 3235–3247 (2016). https://doi.org/10.1109/TNET.2015.2512301
24. Yi, S., Hao, Z., Qin, Z., Li, Q.: Fog computing: platform and applications. In: 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb), pp. 73–78, November 2015. https://doi.org/10.1109/HotWeb.2015.22
25. Qu, Y., Zhang, J., Li, R., Zhang, X., Zhai, X., Yu , S.: Generative adversarial networks enhanced location privacy in 5G networks. Sci. China Inf. Sci. (2020)