Hindawi
Mobile Information Systems
Volume 2017, Article ID 7251395, 7 pages
https://doi.org/10.1155/2017/7251395

Research Article

Location Privacy Protection Based on Improved K-Value Method in Augmented Reality on Mobile Devices

Chunyong Yin, Jinwen Xi, and Ruxia Sun

School of Computer and Software, Jiangsu Engineering Center of Network Monitoring, Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology, Jiangsu Key Laboratory of Meteorological Observation and Information Processing, Nanjing University of Information Science & Technology, Nanjing 210044, China

Correspondence should be addressed to Ruxia Sun; src@nuist.edu.cn

Received 29 October 2016; Accepted 27 December 2016; Published 13 February 2017

Academic Editor: Jaegeol Yim

With the development of Augmented Reality technology, the application of location based service (LBS) is more and more popular, which provides enormous convenience to people's life. User location information could be obtained at anytime and anywhere. So user location privacy security suffers huge threats. Therefore, it is crucial to pay attention to location privacy protection in LBS. Based on the architecture of the trusted third party (TTP), we analyzed the advantages and shortages of existing location privacy protection methods in LBS on mobile terminal. Then we proposed the improved K-value location privacy protection method according to privacy level, which combines k-anonymity method with pseudonym method. Through the simulation experiment, the results show that this improved method can anonymize all service requests effectively. In addition to the experiment of execution time, it demonstrated that our proposed method can realize the location privacy protection more efficiently.

1. Introduction

Augmented Reality technology, called AR, is a kind of technology that real time calculates the position and angle of the camera image and allows adding the corresponding image, video, 3D model generated by a computer to the reality [1]. The concept of AR was proposed in 1990 by Thomas Caudell, an employee of Boeing [2]. After many years of technological development, AR has evolved through different stages and now it is becoming one of the commonly used technologies. Today one of the commonly accepted definitions of AR is given by Ronald Azuma [3], which says that Augmented Reality contains three aspects:

(1) Combination of virtualness and reality

(2) Real-time interactivity

(3) Registration in 3D

With the development of wireless sensor technology and advanced devices, it is possible to get the accurate personal location information of the mobile terminal user anytime and anywhere; therefore, location based service (LBS) is a new class of applications. Location based service is one of the common services provided by AR, which accesses to the position information related to the user through mobile wireless network or external positioning mode [4]. With the information, it adds the value of services. LBS normally consists of location system, mobile devices, network, and service provider (LBS server). In this service, users send the local position information to LBS server and get the corresponding query results [5]. For example, the user uses the mobile phone to send the information to the server, then the location system acquires the query, and finally the server returns the feedback to the user through network.

There are many categories of services that LBS can provide, including Emergency Services, Communities and Entertainment, Information and Navigation, Tracking and Monitoring, and Mobile Electronic Commerce. In 2003, CSTB (Computer Science and Telecommunications Board) in the "IT Roadmap to a Geospatial Future" pointed that LBS would be a very important part of future computing

environment, with the gradual maturity of technology, and it would be infiltrated into all aspects of the future life. The ABI research of market research firm forecasted that the global number of people enjoying location based services from 1.2 million in 2006 would increase to 31.5 million in 2011. And now, the number is much more than that.

The head mounted display is used as a fusion display device in early Augmented Reality system, which limits the scope of the user's activities to a certain extent and is not conducive to the outdoor environment. With the rapid development of mobile devices and network technology, the application of Augmented Reality technology in mobile terminals has been involved in many fields, such as games, social networks, e-commerce, and personal health care. So it is very important to classify these services that are achieved from those fields. KNN algorithm, SVM algorithm [6, 7], Hoeffding-ID data-stream [8], and so on are the common classification algorithms. At the same time, feature selection is also necessary in the process of classification. Some effective feature selection algorithms are introduced in [9].

The application of AR is becoming more and more extensive with the development of AR and LBS technology. In other words, a technology boom takes place in the case of AR and LBS is one of the most widely used services of AR. For example, Pokémon GO is the popular game based on AR, which springs up around the world. However, if users do not take the appropriate security measures and develop these technologies unlimitedly, widely known serious privacy threats will be presented to them. The important threats are the leak of service content and location privacy. Service content threat is the potential exposure of service users. For example, a user searches the Internet regularly; he does not want to be identified as the subscriber of some LBS. User's location is disclosed in the service request, which results in the leak of location privacy. Some sensitive information may be revealed such as health conditions and lifestyles. The leak of location privacy restricts the use of LBS, which has also become the bottleneck of the development of LBS and AR technology [10].

2. Related Work

User location privacy [11] is a kind of special information privacy, and it still belongs to the category of information privacy. Information privacy refers to sharing information with others in a certain period of time, in a place or in some way defined by individuals or institutions, and location privacy refers to preventing the attacker from accessing to the user's location information in some way as far as possible. In LBS, sensitive attribute data can be the time information and spatial information related to the users and the content of the service request contains many respects, such as health care information and property information. The attackers can use this information to infer the user's travel patterns, hobbies and interests, and other personal privacy information. Location privacy threat refers to, under unauthorized circumstance, the fact that attacker tracks the original position information through location device and technology and infers the privacy information related to user location through reasoning [12].

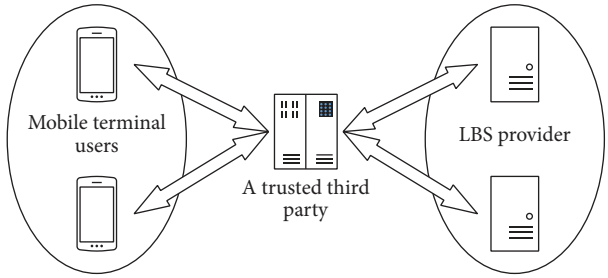

Figure 1: The trusted third party model.

Location privacy protection method mainly refers to the fact that the user provides false user location privacy information or anonymous user's identity information and location information to the server in the process of location service. The model of location privacy protection is divided into 2 categories, which are trusted third party (TTP, shown in Figure 1) and free trusted third party (FTTP) [13]. This paper only discusses the previous class method.

It is easy to understand the location privacy protection based on TTP model; as a result, it is very common. Generally speaking, a reasonable discount is proposed among the efficiency, accuracy, and privacy. In order to solve the problem of location privacy leakage, many researchers try to balance the service quality and privacy protection, which means the best service with least location privacy exposure.

Today, we have already proposed a lot of privacy protection methods, like pseudolocation method, pseudonym method, k-anonymity method, and other methods based on it, such as personalized k-anonymity.

2.1. Pseudolocation Method. Pseudolocation method is another location privacy protection method, which is used to protect the user's identity. This technology generalizes the user's true location and uses the location space region coordinates to represent the user's true location information [14]. There are two situations for this method to realize the location privacy protection. The first one is that the user forms the pseudolocation by himself, after putting forward the service request, and sends it with his real location to the LBS provider. Therefore, the attacker cannot discriminate the pseudo and real location, which protects the user's location privacy. The other situation is that when putting forward the service request, the user only sends one specified pseudolocation. When the server receives the location, it will increase the resent adjacent inquiry and send the results to the client. So the user can find the requisite answer from the results. In this way, the location privacy can still be protected because the real location information of the user is not acquired by the attacker. But the defect of this method is still obvious. In this method, the space of user acts is restricted. And the level of location privacy protection is not fixed, which is proportional to the distance between the pseudo- and real locations. In other words, the level of privacy protection will

be low if the pseudolocation is close to the real location of the user and vice versa.

2.2. Pseudonym Method. Pseudonym method [15] can realize the protection of user identity. That is to say, the user sends a service request through a false identity instead of the true identity and confuses the relationship between the position information and user identity information. In this method based on TTP model, TTP is the simplest intermediary entity between the user and the LBS provider. If the request is accepted, the request will be sent to the LBS provider; at the same time, the real ID will be changed to a pseudo-ID. In this way, the real ID is hidden for the provider. Even if the attacker obtains the accuracy location information, the exact interconnection between the user's location information and real ID still cannot be established. Through the pseudo-ID, the real ID could be concealed by user, which realizes the location privacy protection. Although this method can realize privacy protection to a certain extent, its shortage still exists. The server records all information of user's request and corresponding IP address, which will lead to the location privacy leak.

2.3. K-Anonymity Method. There is another location privacy protection method called k-anonymity method. Its idea comes from the k-anonymity model, which was proposed by Latanya Sweeney of the University of Carnegie Mellon in the United States. K-anonymity method was firstly proposed by Gruteser and Grunwald [16]. Before sending to the LBS provider, user deletes the personal information and publishes hypoaccurate data, which induces the fact that each record has identical quasi-identifier value with other $k - 1$ record in the data list. The identity of each user is accurately identified as $1/K$ under the condition of the same probability. K-anonymity method realizes the location privacy. But the restriction of k-anonymity method is that there is no protection mechanism for leak of sensitive attribute data, and there is not any constraint for sensitive attribute data in this method. It is easy for the attacker to infer the individual corresponding sensitive attribute data and identify the relationship between data and individual through the background information, which leads to the location privacy leak [17].

2.4. Personalized k-Anonymity Method and Other Methods. Because of the defect of k-anonymity method, other methods have been proposed to improve k-anonymity model. For example, A. Machanavajjhala proposed l-diversity model based on k-anonymity model. But this model is only suitable for dealing with classification sensitive attribute data instead of numerical sensitive attribute data. P-sensitive k-anonymity model could lose a lot of information usability in some data set and cannot resist the skewed attack and similarity attack to the sensitive attribute data. After P-sensitive k-anonymity model, (α, k)-anonymous model and (k, e)-anonymous model have the same defect. T-closeness frame can fix the skewed attack and similarity attack to the sensitive attribute data. But it reduces the usability of published data [18].

Personalized k-anonymity method was proposed by Gedik et al. [19, 20]. In this method, each user can define the desired anonymous level. The desired privacy level of every user is different, so personalized k-anonymity method is very popular. This method can provide different level of privacy protection to sensitive attribute data, which will decrease the data lost from the unified anonymous. But there is a defect in this method that the proportion of anonymous information will decrease when the K-value increases.

3. Improved K-Value Location Privacy Protection Method

In LBS, in order to achieve the protection, there are three main models: (1) noncooperative model; (2) peer-to-peer cooperative model; and (3) TTP model. This paper proposes the improved K-value location privacy protection method that is based on the TTP model, which will realize user location anonymous, service request anonymous, and feedback to the user. This model connects the user and LBS provider. Through the analysis, we found that all kinds of location privacy protection methods mentioned above based on TTP model have some disadvantages. For example, users need to customize the value of K when they use personalized k-anonymity method. But it is hard to choose the suitable value of K. The suitable value of K has a close connection with the quality of LBS service and the request of privacy protection. Therefore, we propose the improved K-value location privacy protection method based on the previous location privacy protection method.

3.1. Frame Model of Improved Method. Improved K-value location privacy protection method is a special location privacy protection method. In this system, the maximum and minimum values of K are needed to be set and there is no other default status. The location privacy level is obtained from the feedback learning of the ideal users. The value of K will be adaptive with the feedback and finally close to the requests of users. So we also call this method improved adaptive k-anonymity location privacy protection method. The frame model of the improved K-value location privacy protection method is shown in Figure 2.

3.2. Algorithms and Procedure of Improved Method

Algorithms. Set $k_{\min}$ as the minimum value of K and $k_{\max}$ as the maximum value of K; set $k_{\min} = 2$ and $k_{\max} = 8$.

(1) The user sends the service request to the server;

(2) The trusted third party receives the service request in the transmission process;

(3) Controller defines the level of privacy;

(4) Controller defines the value of K;

(5) If $K \in (k_{\min}, k_{\max})$;

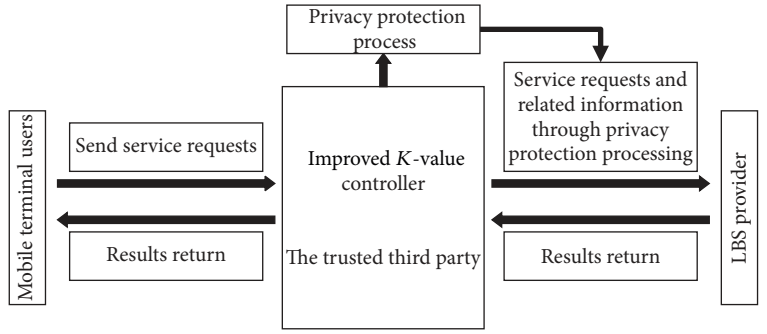

Figure 2: The frame model of the improved K-value location privacy protection method.

(6) The trusted third party processes the privacy protection with improved k-anonymity method and pseudonym method;

(7) Else;

(8) If $K < k_{\min}$;

(9) The trusted third party processes the privacy protection with k-anonymity method;

(10) Else;

(11) If $K > k_{\max}$;

(12) The trusted third party processes the privacy protection with pseudonym method;

(13) End if;

(14) End if;

(15) End if.

Summing up, the algorithm is summarized into a figure:

$$\text{process method} = \begin{cases} \text{improved } k\text{-anonymity method and pseudonym method}, & K \in (k_{\min}, k_{\max}) \\ k\text{-anonymity method}, & K < k_{\min} \\ \text{pseudonym method}, & K > k_{\max} \end{cases} \quad (1)$$

Procedure. From the above algorithms, algorithm procedure can be divided into three parts. (1) If the value of K is higher than $k_{\max}$, the trusted third party will adopt the pseudonym method to anonymize the user's location information. Here the real id will be replaced by the pseudo id and the pseudo id will be saved in the trusted third party database list with the real id and other detailed information of the user. When the trusted third party receives the result from the LBS provider and gets ready to send it to the mobile terminal, this system will check the corresponding real id of user in this list connected with the pseudo id, and then all primal data will be feedback to the mobile terminal user. (2) If the value of K is lower than $k_{\min}$, the trusted third party will adopt the k-anonymity method to anonymize the user's location information. The trusted third party will transmit the result to the LBS provider and send the feedback that received from the LBS provider to the mobile terminal user. (3) If the value of K is located in the set range, the trusted third party will adopt the k-anonymity and pseudonym methods to anonymize the user's location information. The trusted third party will send service request to the LBS provider, who will answer the request and return the results to the mobile terminal user.

In this algorithm, the range of values of $k_{\max}$ and $k_{\min}$ are as follows: the privacy disclosure threshold given by the data publisher is $P_{\max}$, the privacy disclosure probability of K-anonymity table is P, T is original data table, and T' is the K-anonymity table. The victim is U and the privacy attribute of value is S_u; each tuple with U is denoted as IG_u and $|\mathrm{IG}_u| = e$. The number of S_u that appears in IG_u is denoted as $|S_u| = f$; then the connecting candidate set of U is denoted as C_u and $|C_u| = g$.

Then, the probability of privacy disclosure of the individual attacked party U can be expressed as

$$P(U) = \frac{g^e - g^{e-f}(g-1)^f}{g^e} = 1 - \left(1 - \frac{1}{g}\right)^f. \quad (2)$$

In (2), $g^e - g^{e-f}(g-1)^f$ is the possible situation with some kind of special privacy and g^e is all. When the maximum number of replications of the sensitive attribute values in the tuple is l, according to $f \le l$ and $g \ge e \ge k$, then

$$P(U) = 1 - \left(1 - \frac{1}{g}\right)^f \le 1 - \left(1 - \frac{1}{k}\right)^l. \quad (3)$$

If $1 - (1 - 1/k)^l \le P_{\max}$, then $1 - (1 - 1/k)^l \ge 1 - P_{\max}$, and finally

$$k \ge \frac{1}{1 - (1 - P_{\max})^{1/l}}. \quad (4)$$

Therefore,

$$k_{\min} = \frac{1}{1 - \left(1 - P_{\max}\right)^{1/l}}. \quad (5)$$

Next, we use the identification metric C_{DM}. C_{DM} is represented as $C_{\mathrm{DM}} = \sum_{j=1}^{N} |\mathrm{IG}_j|^2$, where N is the number of tuples and $|\mathrm{IG}_j|$ is the scale of the j tuple in the anonymous table. Because $k \le |\mathrm{IG}_j| \le 2k - 1$, $k \le C_{\mathrm{DM}} \le 2k - 1$, when given $C_{\mathrm{DM}_{\max}}$ ($C_{\mathrm{DM}_{\max}} \ge 2k - 1$), then

$$k_{\max} \le \frac{C_{\mathrm{DM}_{\max}} + 1}{2}. \quad (6)$$

4. Experiment and Performance Analysis

Due to the limitation of the actual environment, we analyze and demonstrate the privacy protection methods through the simulation experiment.

4.1. Experimental Data Sets and Parameter Values. In this simulation experiment, we think that the automobiles along the road send the service request to the server, which are replaced by the moving object generators. The service request is based on the location information of the moving object generator. We use OPEN GL to simulate the national mapping map, which is provided by US Geological Survey. This map utilizes the spatial data transmission standards.

Experiment circumstance is Intel® Core™ i3-2310M 2.10 GHz for CPU, 6 GB for memory in Windows 10 Multiple Editions. Programming circumstance is Eclipse + Hibernate + SQL Server 2014. In this experiment, 500 moving object generators were used to simulate the automobile along the road and 580-service-request information was received. K-value was set as 2, 3, 4, 5, 6, 7, and 8.

4.2. Performance Analysis. In order to measure the results of the experiment, we adopt the anonymized success rate. The anonymized success rate is the ratio of the number of requests anonymized by the trusted third party to the total number of requests sent to the trusted third party, which is an important parameter for performance evaluation of privacy protection methods. It can reflect the response capability of the location privacy protection algorithm to the user's service request; the higher the value of the algorithm is, the better the capability will be.

4.3. Experiment Results. In the simulate experiment, we input different K-values in order to check the working of the algorithm in different contexts. With the value of K changing constantly, it is discovered that the number of information anonymized using different methods is different. When the value of K is small, we find that the most information is anonymized with k-anonymity method and only a bit of information is anonymized by pseudonym method. However, with the enlargement of K-value, more and more information will be anonymized with pseudonym method while less and less information will be anonymized by k-anonymity method.

Table 1: Number of information anonymized by k-anonymity method and pseudonym method.

K-value	2	3	4	5	6	7	8
The number of messages using k-anonymity method	503	432	360	293	222	156	72
The number of messages using pseudonym method	77	148	220	287	358	424	508

Table 2: Execution time of anonymous process using different methods.

K-value	2	3	4	5	6	7	8
The execution time of improved method	1.30 s	1.54 s	1.79 s	2.01 s	3.48 s	4.05 s	5.67 s
The execution time of personalized k-anonymity method	1.29 s	1.59 s	1.87 s	2.43 s	4.11 s	5.30 s	7.03 s

That is to say, when the value of K is less, the k-anonymity method will be used more and as the value of K increases, the use of pseudonym method will get increased. The number of information anonymized by k-anonymity method and pseudonym method is recorded in Table 1.

In order to reflect the efficiency of anonymous algorithm that we proposed, we record the execution time of anonymous process using different methods, which is the time of anonymous process for all inquiry requests from a certain scale of mobile uses. If the execution time is shorter, the anonymous algorithm is more efficient. Otherwise, the efficiency of the anonymous algorithm is worse.

In this experiment, we compare the execution time of improved K-value location privacy protection method and personalized k-anonymity method. From the results, it is discovered that when the value of K is small, the execution of time is almost the same for both methods. However, with the enlargement of the value of K, we realize that the execution time of personalized k-anonymity method is significantly longer than the execution time of the previous, which is owing to its much deeper refinement to the data and bigger searching space. In this execution of the personalized k-anonymity method, after each refinement, the restraint of every new anonymous group is needed to be calculated and the sensitive attribute generalization will also be undertaken by it, which costs longer execution time. The execution time of anonymous process using improved method and personalized k-anonymity method is recorded in Table 2.

Figures 3 and 4 are used to compare the results of the experiment more directly.

In Figure 3, we can see that the number of information anonymized by k-anonymity method will decrease with the enlargement of K-value, which is opposite to the number of information anonymized by pseudonym method.

From Figure 4, we see that the execution time of our proposed method is less than the personalized k-anonymity

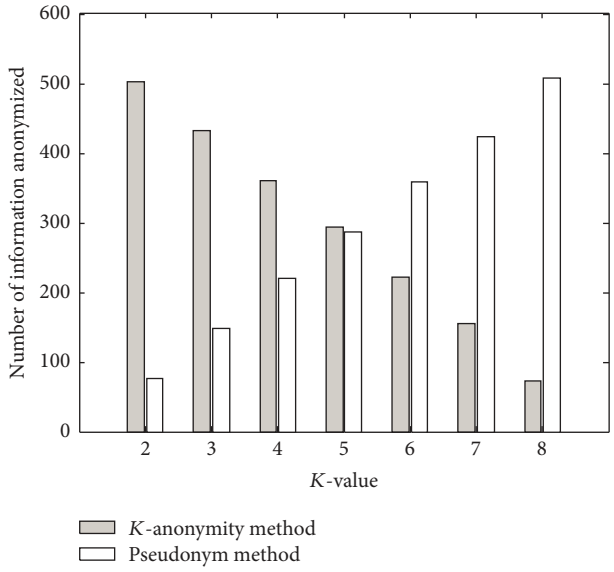

Figure 3: Number of information anonymized by k-anonymity method and pseudonym method.

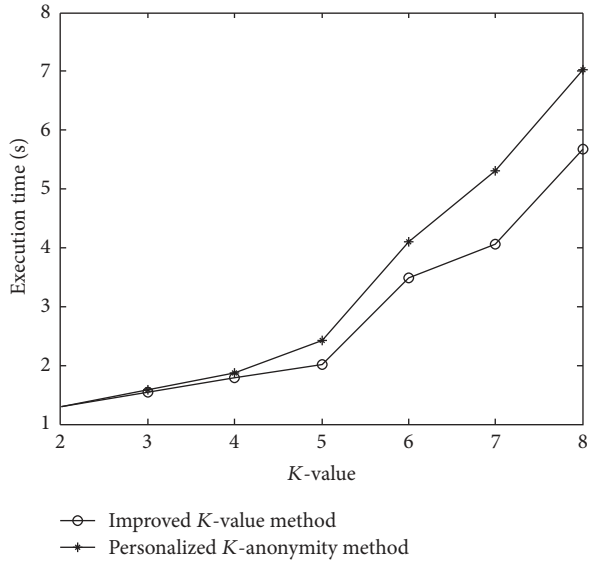

Figure 4: Execution time of anonymous process using different methods.

method, which means that the efficiency of this improved method is higher.

5. Conclusions

In this paper, we analyze the location privacy protection method in Augmented Reality, which is worth being paid attention to. It is crucial for privacy protection and data quality to choose reasonable K-values, so we propose the improved K-value location privacy protection method based on the previous methods. This method could define the value of K according to the level of privacy protection. Then different privacy protection methods are adapted according to the value of K to process the user's location privacy. Through the simulation experiment, the method we propose can anonymize all service requests effectively with shorter execution time, which realizes the location privacy protection more efficiently. However, the location privacy protection method is not perfect in Augmented Reality and it needs further study on the relevant issues.

Competing Interests

The authors declare that they do not have any conflict of interests related to this work.

Acknowledgments

This work was funded by the National Natural Science Foundation of China (61373134). It was also supported by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD), Jiangsu Key Laboratory of Meteorological Observation and Information Processing (KDXS1105), and Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology (CICAEET).

References

[1] P. Milgram and F. Kishino, "Taxonomy of mixed reality visual displays," *IEICE Transactions on Information and Systems*, vol. E77-D, no. 12, pp. 1321–1329, 1994.

[2] E. Olshannikova, A. Ometov, Y. Koucheryavy, and T. Olsson, "Visualizing Big Data with augmented and virtual reality: challenges and research agenda," *Journal of Big Data*, vol. 2, no. 1, pp. 1–27, 2015.

[3] Wikipedia, "Augmented reality," http://en.wikipedia.org/wiki/Augmented_reality.

[4] M. Deidda, A. Pala, and G. Vacca, "An example of a tourist location-based service (LBS) with open-source software," *Applied Geomatics*, vol. 5, no. 1, pp. 73–86, 2013.

[5] C. Yin and J. Xi, "Maximum entropy model for mobile text classification in cloud computing using improved information gain algorithm," *Multimedia Tools & Applications*, 2016.

[6] B. Gu, V. S. Sheng, K. Y. Tay, W. Romano, and S. Li, "Incremental support vector learning for ordinal regression," *IEEE Transactions on Neural Networks & Learning Systems*, vol. 26, no. 7, pp. 1403–1416, 2015.

[7] B. Gu, V. S. Sheng, Z. Wang, D. Ho, S. Osman, and S. Li, "Incremental learning for ν-support vector regression," *Neural Networks*, vol. 67, pp. 140–150, 2015.

[8] C. Yin, L. Feng, and L. Ma, "An improved Hoeffding-ID data-stream classification algorithm," *Journal of Supercomputing*, vol. 72, no. 7, pp. 2670–2681, 2016.

[9] C. Yin, L. Ma, and L. Feng, "A feature selection method for improved clonal algorithm towards intrusion detection," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 30, no. 5, Article ID 1659013, 2016.

[10] X. Li, M. Miao, H. Liu, J. Ma, and K.-C. Li, "An incentive mechanism for K-anonymity in LBS privacy protection based on credit mechanism," *Soft Computing*, 2016.

[11] I. Memon, "Authentication user's privacy: an integrating location privacy protection algorithm for secure moving objects in

location based services," *Wireless Personal Communications*, vol. 82, no. 3, pp. 1585–1600, 2015.

[12] Y. Sun, L. Yin, L. Liu, and S. Xin, "Toward inference attacks for k-anonymity," *Personal and Ubiquitous Computing*, vol. 18, no. 8, pp. 1871–1880, 2014.

[13] M. Bialke, P. Penndorf, T. Wegner et al., "A workflow-driven approach to integrate generic software modules in a Trusted Third Party," *Journal of Translational Medicine*, vol. 13, article 176, 2015.

[14] M. Uzielli, F. Catani, V. Tofani, and N. Casagli, "Risk analysis for the Ancona landslide—I: characterization of landslide kinematics," *Landslides*, vol. 12, no. 1, pp. 69–82, 2015.

[15] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular Ad-Hoc networks," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 160–171, 2010.

[16] B. Kenig and T. Tassa, "A practical approximation algorithm for optimal k-anonymity," *Data Mining and Knowledge Discovery*, vol. 25, no. 1, pp. 134–168, 2012.

[17] P. Belsis and G. Pantziou, "A k-anonymity privacy-preserving approach in wireless medical monitoring environments," *Personal and Ubiquitous Computing*, vol. 18, no. 1, pp. 61–74, 2014.

[18] B. Zhou and J. Pei, "The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks," *Knowledge and Information Systems*, vol. 28, no. 1, pp. 47–77, 2011.

[19] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1–18, 2008.

[20] Z. Xia, C. Yuan, X. Sun, R. Lv, D. Sun, and G. Gao, "Fingerprint liveness detection using difference co-occurrence matrix based texture features," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 11, no. 11, pp. 1–16, 2016.