Bulletin of Electrical Engineering and Informatics
Vol. 4, No. 4, December 2015, pp. 345~354
ISSN: 2089-3191

Location-Based Services and Privacy Protection under Mobile Cloud Computing

Yan Yan*[1], Hao Xiaohong*[2], Wang Wanjun[3]
[1]School of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou, China
[1,2]School of Computer and Communication, Lanzhou University of Technology, Lanzhou, China
[3]Information Engineering College, Lanzhou University of Arts and Science, Lanzhou, China
e-mail: yanyan@lut.cn[1]; wangwanjun1@163.com[2]

Abstract

Location-based services can provide personalized services based on location information of moving objects and have already been widely used in public safety services, transportation, entertainment and many other areas. With the rapid development of mobile communication technology and popularization of intelligent terminals, there will be great commercial prospects to provide location-based services under mobile cloud computing environment. However, the high adhesion degree of mobile terminals to users not only brings facility but also results in the risk of privacy leak. The paper introduced the necessities and advantages to provide location-based services under mobile cloud computing environment, stressed the importance to protect location privacy in LBS services, pointed out new security risks brought by mobile cloud computing, and proposed a new framework and implementation method of LBS service. The cloud-based LBS system proposed in this paper is able to achieve privacy protection from the confidentiality of outsourced data and integrity of service results, and can be used as a reference while developing LBS system under mobile cloud computing environment.

Keywords: *location-based services; location privacy; mobile cloud computing; ciphertext-policy attribute-based encryption*

1. Introduction

With the rapid development of mobile communication technology and the growing popularity of intelligent terminals, there is an urgent need to get information and services from the Internet at anytime and anywhere even during movement. The urgent needs of information and services promoted the convergence of Internet technology and mobile communication technology, and finally formed the Mobile Internet. Among the wide variety of Mobile Internet services, location-based services (LBS) are the most widely used one. It can provide many personalized services for mobile users according to their location information. Users can not only access to basic geography-related services, but also achieve communication, purchasing and sharing based on social network, as well as get news, arrange dating, release and search information during movement [1].

In the era of Mobile Internet, cell-phone is much more than a tool for communication; it has already become an "organ" of our body, and has even become an indispensable part of people's social relationships. However, the high adhesion degree of mobile terminals to users not only brings facility but also bring new security risks. Physical location and trajectory data of mobile user contains a large number of personal privacy information. If the specific location information of user has been leaked while using the LBS services, it may disclosure some privacy information of user, such as interests, habits, health status, political affiliation, even cause huge loss of personal property and security.

The paper started from the application perspective of mobile cloud computing, analyzed the advantages and necessity to provide LBS services based on mobile cloud computing, introduced the traditional protection methods of location privacy and pointed out the new security risks to LBS system brought by mobile cloud computing. In order to solve the above problems, the paper proposed a systematic framework of LBS system and described the realization process of LBS business based on mobile cloud computing.

Received February 3, 2015; Revised June 22, 2015; Accepted July 17, 2015

2. Location-Based Services under Mobile Cloud Computing

Mobile Internet provides good communication means from terminal users to data center, but with the comprehensive promotion of smart phones and fast increasing of various applications, computation work for mobile terminals is also growing, that is a big challenge for mobile terminals which has limited computing ability and storage resources. For location-based services, a large number of location information and trajectory data has been generated every day, the amount of data from transit hub, subway station, airports and other densely populated areas reach millions of magnitude daily. How to analyze and query the large number of location information and trajectory data? How to deal with the large number of queries and to provide real-time and quality service? These are the reality problems location-based services providers have to face.

The continued development and integration of Cloud Computing and Mobile Internet result in a new application model—Mobile Cloud Computing (MCC). The emergence of MCC provides a new business model for LBS services, LBS providers do not have to invest a lot of money and equipment to improve their storage and query capabilities, and do not necessarily need to have their own cloud platform, but to outsource their data and services on to the cloud computing platform and achieve massive data storage and query services by cloud computing service providers. In the year 2011, the leader company of wireless communication in United States, AT & T, announced the start of its platform services created for location-based information based on cloud computing [2]. December 2011, deCarta company launched its cloud-based LBS service platform [3]. September 2012, Baidu announced a new platform-level service for LBS developers, which called "LBS.Cloud" [4]. In 2013, TomTom began to build its cloud-based LBS platform [5]. All of these marked the arrival of the cloud computing era for LBS services.

Developing location-based services on cloud computing platform has many advantages. Firstly, compared with desktop computers, the significant problem of mobile terminal is lacking of resources, mainly reflected in less screen area, limited computing capability, shortage of storage resource and restriction of battery capacity etc. The LBS system based on mobile cloud computing breaks through the hardware limitations of terminals and transfers complex calculation and data query processing from local to the cloud platform [6]. The only thing users need to do is to have a smart mobile device to send commands to the "cloud" and receive data from it. Besides, users can use the computing resources, storage space and variety of software applications from cloud service providers to achieve mobile navigation, portable Yellow Page, location advertising, mobile emergency, etc [7]. Thereby, the computing pressure on client and development costs has been reduced so that the performance bottlenecks of user terminal will gradually disappeared. Secondly, as a new method of shared infrastructure, cloud computing make unified management and scheduling on large number of hardware and software resources, and form a resource pool to provide services to users according to their demand. By the means of application hosting, LBS providers can outsource their data and services to the cloud computing platform without investing a lot of money and equipment to improve the storage and query capabilities, so that the operation and management costs will be reduced. Thanks to the huge resource pool supplied by cloud computing, it not only solved the massive data storage problem, maintenance pressure and bottlenecks caused by high concurrent retrieval, but also improved the service quality and scalability of system, facilitated the access of location-based services.

3. Privacy Protection of LBS System

Location-based services have become an important component of future computing environment, and have already seamlessly integrated into people's daily lives. However, the high adhesion of mobile terminals to users not only brings facility, but also brings the risk of privacy leak. During the process of location-based services, the physical location information of user has been got or gathered and reported to the LBS service providers, which will carry out the inquire services combined with user's location information and specific requests, finally the service results will be send back to users from LBS service providers. If a malicious attacker intercepted the LBS service request, and finally obtained the original location information by calculating or reasoning their position information, that will result in serious threat on personal security and vital interests. As the physical location and trajectory data of mobile user contains a

lot of personal privacy information, once be disclosed, it will lead to the disclosure of user's interests, habits, health status, political affiliation and other personal privacy information [8]. For example, if a user frequently visits hospitals or clinics in a certain period of time, the attacker can deduce that he is likely to suffer a disease. If a user start from place A and arrive place B every morning within a fixed period of time, and from place B return to place A every afternoon within a fixed period of time, an attacker could easily determine that place A may be the user's home address and place B may be the work unit. The U.S. Fox company has reported a case that someone uses GPS trajectory data to track his ex-girlfriend and carry out revenge [9]. Reference [10] also reported a company monitors the whereabouts of their employees with cell-phones equipped with GPS. All of these cases caused by exposure of location and trajectory information remind us that location privacy problem has already become the most urgent task in LBS system and it is the high time to solve this problem.

3.1. Location Privacy of Traditional LBS System

Protection of location privacy is an important research content of LBS technology, a physical location which has been frequently visited in terms of time or track is likely to expose the personal privacy of user. Through the analysis of user's location and trajectory, attackers are not only able to find out the current positions of users, what places they have visited in the past, but also able to infer the home addresses, places of work, or even deduce the living habits, income levels, health status, behavior patterns and other private information of users through their daily trajectory. Therefore, location privacy protection of LBS system is not only to ensure the physical location information of LBS service query, but also to protect the trajectory and history records not be used by attackers illegally [11].

In order to protect the location privacy in an instantaneous query, the most frequently used method is to publish a pseudonym or use spatial and temporal cloaking to prevent or reduce the recognizability of positional information. The former send a false position to the location database server in order to protect the real location information of user, the degree of protection on privacy and quality of service is related on the distance between false position and real position. Representative algorithms like the SpaceTwist method proposed in reference [12] and Casper method proposed by reference [13]. Spatial and temporal cloaking use a spatial or temporal region to represents the precise location of user, attackers only know the user located in a spatial or temporal region, but cannot determine the specific location within the entire region. Marco Gruteser is the first one to use the concepts of K-anonymity in location privacy protection, and proposed location-based K-anonymity method in reference [14]. The main idea is to include at least *k* users in a certain region (called anonymous region) and the users cannot be identified by their ID number, so that an adversary may manage to identify that a spatial region has been visited by *k* different people, but it will not know who was there at time of the service request. On the basis of *k*-anonymity, many other algorithms have been proposed, such as anonymous method based on spatial division [15], K-anonymity based on Hilbert [16] and location-based dynamic anonymity [17]. Trajectory is the sequence of position information of moving objects sorted according to time. By continuously intercepting the user's location information, the attacker can finally obtain the trajectory of user by linking the position information of user in different time. Though some location protection methods have been used, it does not mean that protection of location information equals to the protection of real-time trajectory information. Reference [18] has pointed out that when using the location-based K-anonymity model for location privacy protection, the position and size of anonymous box will be continuously updated according to the user's different queries. Joining these anonymous boxes up according to their sending time, it is possible to get the path of moving objects substantially. Currently, the protection of trajectory privacy is still in a primary stage, some existing methods are mainly focused on adding fake trajectories to disturb the original ones [19] [20], changing the sampling points on the trajectory into the generalization anonymous region [21] [22], or not to publish frequently visited sensitive positions on the trajectory so as to achieve the purpose of trajectory privacy [23] [24].

3.2. New Security Problems Brought by Mobile Cloud Computing

The combination of cloud computing and mobile internet will not only face the security threats from traditional internet and mobile communication network, but also introduced the security risks of cloud computing technology, which brings unprecedented security challenges to

user's data. The right of ownership and management of user data will be separated in the model of mobile cloud computing, LBS service providers will store and manage their geographic data and information through the cloud platform, end-user will query, access and transmit this information via the mobile internet. How to ensure that the cloud computing service provider has did correct storage, access, management and destruction on the data of LBS provider? How to prevent user data from been lost, stolen, tampered during the network transmission? These are all the major problems location privacy protection has to deal with under the mobile cloud computing environment.

From the side of mobile terminals, as a part of modern life, the high sticky degree of mobile terminals to users is likely to attract eavesdropping and surveillance problems. The operation systems of intelligent terminals nowadays are not perfect, and there are many security vulnerabilities yet to be resolved. As the main entrance of applications under mobile cloud computing environment, browsers still have some software vulnerabilities. What's more, the users of mobile Internet are lack of safety awareness compared to PC users while using cloud services. It is easy to be infected with the virus or intrusion while receiving SMS, MMS or browsing mobile web, downloading and installing software, result in data leakage, equipment damage and economic losses. In recent years, some famous manufacturers of mobile phones are facing a crisis of confidence. It is reported that some intelligent terminals or third-party applications installed on it will collect the location information of user forcibly without authorization, and periodically send the information to the manufacturer's data center to analyze the behavior of mobile users, or release it to other organizations for commercial applications [25].

From the side of network, the nature of wireless transmission decided that mobile cloud computing has some security risks in connection authentication and data protection, etc. Among them, access to the network illegally by breaking the wireless interface and monitoring, stealing, attacking the message transmitted on the air interface is particularly prominent. Therefore, on one hand, the cloud-based LBS system needs to deal with the leakage of user's location information caused by illegal intercept and capture of service requests during the transmission process. On the other hand, it also has to consider the situation that illegal attackers will steal or tamper the information return from cloud platform in order to backward reasoning the user's private information.

The new security risks to LBS system brought by mobile cloud computing are mainly focused on the cloud. Firstly, virtualization technology brings scalable features to cloud computing, but virtual machines of different users might be running on the same physical storage device, if the software of virtual machine or the physical host has some problems, the data of LBS provider may be accessed by other users running on the same physical storage devices leading to the disclose of user's privacy. Secondly, the data of different users is stored and managed centrally under the cloud computing environment. How to ensure the security management of cloud platform and prevent intentional or unintentional leakage of data from the cloud platform belonged to the LBS providers? Finally, due to the high concentration of information resource, cloud platforms are easily to become the target of hacker attacks, which brings greater security risks to the business and users running on it [26].

4. LBS System and Location Privacy Protection under MCC

4.1. System Structure of LBS under Mobile Cloud Computing

In order to protect the location privacy of user during a LBS service, traditional system adopt TTP-based (trusted third party) structure or distributed point-to-point structure. In the former one, users sent their location information to the trusted third party (called anonymizor), which will converted the accurate location information into an inaccurate location and then sent it to the location service providers, together with the service request of users. Location service providers carried out the retrieval and inquire processing according to inaccurate location information and returned the results to TTP. Finally, TTP filtered the results and returned it to users. It is obviously, the conversion process of location information conducted by TTP have protected the user's location privacy by changing the accurate location information into inaccurate region. The effectiveness and reliability of this kind of privacy protection methods mainly depend on the credibility of the TTP. If the TTP collect or disclose the original location

information of user illegally, the user's personal privacy will be nothing left. In recent years, some scandal events about TTP have been reported, which seriously affected the independence and authority of the third-party institution. In addition, all of the user's service requests are sent to the TTP for centralized processing will make the TTP become the bottleneck of system performance. LBS system with distributed point-to-point structure adopts cooperation strategies between the mobile users and requires mutual trust between user's collaboration. If one user wants to launch a location-based request, he needs to generate a concealed space to replace his accurate location information according to other user's location which have been collected, and then sent the concealed location to the location service provider. Advantage of this kind is that there is no TTP in the system, every node within the system has the ability to complete location anonymity and refinement of query results, which will solve the stress of TTP as the bottleneck of system as well as vulnerable problem, meanwhile, there is no need to worry about the risk of user's location information be leaked by the third parties.

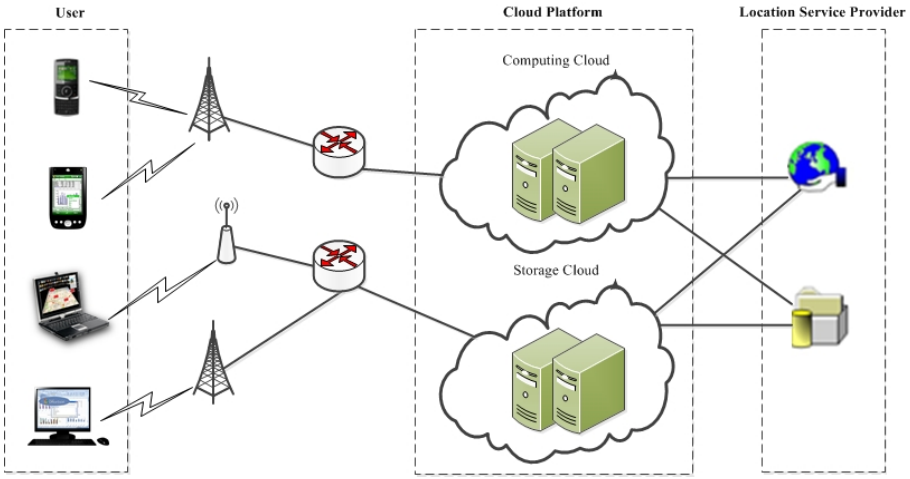

Figure 1. Systematic structure of LBS system under mobile cloud computing

Combined with the concepts such as storage as a service, software as a service, infrastructure as a service, etc., LBS system based on cloud computing can be achieved by variety of ways. For example, according to the idea of infrastructure as a service (IaaS), location service providers can obtain IT resources offered by IaaS cloud service providers according to their needs and deploy their applications and carry out business on it. IT resources mantioned there include: computing resources, storage resources, network resources, middleware resources, database resources, etc. Specifically, location service providers can rent the storage and database resources supplied by IaaS cloud service providers to place and manage their GIS data, take use of the computing resources, network resources and middleware resources supplied by IaaS cloud service providers to complete user access management, authentication, inquire processing, communication, transport and other frequent and complex task. By this way, location service providers avoided continuous investment to the hardware and software, saved a lot of costs on operation and maintenance, once the business needs to be expanded, it is possible to get resources support. The LBS system proposed bu this paper mainly consists of three entities: location service provider, cloud platform and users (shown in Figure 1). Location service provider collect or purchase digital geographic information and form the personalized and customized information after further processing and collating. As a bridge, cloud platform provide storage and computing resources or even application development platform to location service providers on one hand, on the other hand, it provide frequent interaction and inquiry services for the end user. The end user may be mobile phones, PDA or other intelligent terminals access via the mobile internet.

4.2 Process of LBS Services under Mobile Cloud Computing

Implementation process of the LBS services based on mobile cloud computing can be divided into two stages. In the first stage, location service provider has to completed the collection and settlement work of temporal and spatial geographic data in advance, form the final location information that can be published and inquired after pretreatment with their own needs of privacy, and uploaded them to the cloud database platform for storage. This process can be regarded as an “offline” pretreatment (shown in Figure 2). The pretreatment module in “offline” stage is responsible for the division of geographic information data into equivalence classes and synchronization of trajectory data; privacy protection module is responsible for the privacy protection work of the preprocessed data; available measurement module is used to evaluate the availability of data after privacy protection. Because there is not excessive need for the real-time requirements, the "offline" processing stage can give priority to the protection extent of data privacy.

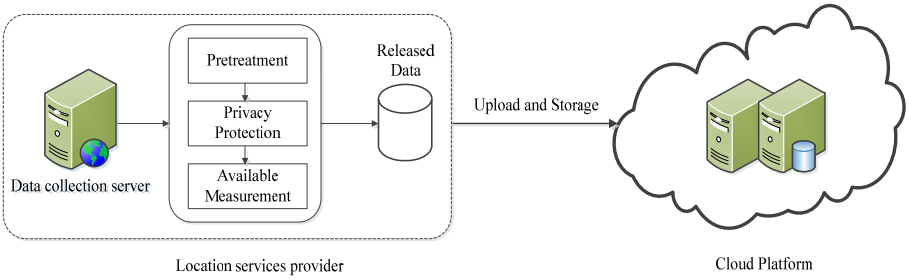

Figure 2. Data processing in “offline” stage

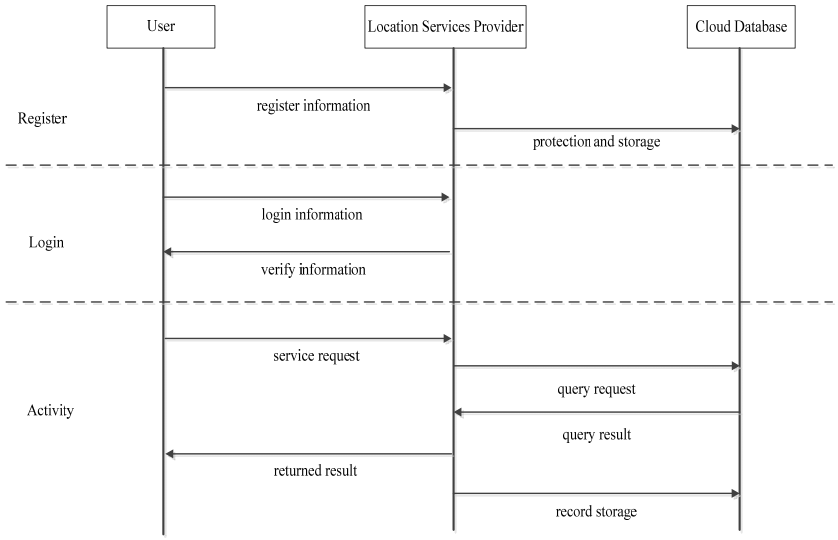

Figure 3. Interactive processing in “online” stage

The real-time interactive processing between location service provider, cloud platform and users belongs to the "online" stage. There are three major steps during the "online" stage: register, login and activity (shown in Figure 3). At first, each user should register a unique account in the location service provider. The register information has been processed in order to protect the privacy information of users and store in the cloud database. Then, users should log in to the location service provider with their ID and password before they use LBS services. During the stage of activity, users send their service request to the location service provider, which contains the physical location information and protection extent request of privacy.

Location service provider then initiate the query progress and get the query result from the cloud database according to certain strategies determined in advance. Final result will be sent back to the user and relevant records will be stored in the cloud database.

4.3 Privacy Protection

LBS system based on mobile cloud computing brings new location privacy issues, which is how to obtain reliable location-based services while using the incredible cloud computing platform at the same time. For the location service providers, some of the customization or fine-grained data are not obtained for free, so location service providers want to protect this kind of data and provide the inquiry of such data only to registered users. In order to protect the security of geographical data and to prevent cloud computing platform and others to collect disclose or leak the outsourced GIS data illegally, location service providers need to carry out some privacy protection process before the data has been outsourced. For the end users, incredible cloud computing platform and attackers bring about potential risks, and may cause illegal disclosure, alteration or deletion to the query results. Therefore, it is necessary for the cloud-based LBS system to ensure the integrity of user's query results, that is to say, the end user can verify that the service result is correct and complete.

Through the above analysis we can conclude that the LBS system based on mobile cloud computing has some security requirements mainly in the following areas:

(1) Avoid illegal collection, crack or leak of outsourced LBS data by cloud storage platform, realize the confidentiality of outsourced LBS data;

(2) Prevent the tamper and delete of some query results by cloud storage platform or illegal attackers, ensure the correctness and completeness of the received results for user;

(3) Avoid the leak of outsourced LBS data caused by conspiracy cooperation of cloud platform or illegal attackers, achieve collusion-resistance.

4.3.1. Privacy Protection of Outsourced LBS Data

In traditional process of data outsourcing, privacy protection methods mainly based on encryption. Original data has been encrypted and sent to the database of outsourced server for storage, users will get an encrypted database from the server when they applied some inquiries and need to decrypt the database and carry out the inquiries on the database after decryption. However, the protection of privacy realized by encryption and the inefficient query caused by encryption is a contradiction, large amount of computing tasks caused by frequent encryption and decryption will bring excessive communication burdens and low efficiency, which is not practical for use. In this paper we designed a new cloud storage solution for LBS outsourced data, using ciphertext-policy attribute-based encryption (CP-ABE) [27] to realize encryption and protection of outsourced LBS information. It can improve the limitation of traditional public-key cryptosystem that only specific users can decrypt the ciphertext, and can fulfill great amount of user's inquery during LBS services.

A ciphertext-policy attribute-based encryption scheme consists of four fundamental algorithms [27]: Setup, Encrypt, KeyGen, and Decrypt.

***Setup*:** The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

Encrypt (PK, M, A)**:** The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message.

KeyGen (MK, S)**:** The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

Decrypt (PK, CT, SK)**:** The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.

Combined with the process of location-based services, the cloud storage solution for LBS outsourced data using ciphertext-policy attribute-based encryption can be achieved as

follows: Firstly, the setup algorithm was carried out by location services provider so as to get the parameters PK and master key MK; then location services provider has to generate the access structure for users according to their set of attributes, and carried out the encryption algorithm on the original geographic information to form the encrypted information, that will be stored on the cloud platform for the later use; after that, location services provider can produce private keys and deliver them to appropriate users by running the key generation algorithm; finally, end users can use the parameter PK got by normal login to the LBS services, encrypted information received from cloud platform and private keys to get the decrypted LBS information eventually by the decryption algorithm.

4.3.2. Privacy Protection of User Information

Traditional verification methods for the integrity of data mainly use the Hash function or digital signature technology. In this paper we proposed another method to achieve confidentiality, completeness and authentication at the same time. It can be described as the following steps.

On the side of transmitter:

***Step 1*:** Use some irreversible encryption methods (for example the Hash functions) to calculate the feature code of data waiting to be sent, in order to verify the completeness of data. This process can be described as $Hash(data) \to F$.

***Step 2*:** The transmitter encrypt the feature code F by his private key SK_c: $encode(F, SK_c) \to C_F$. The new feature code C_F after encryption will be put behind the data waiting to be sent, in order to authenticate the identity of transmitter.

***Step 3*:** The transmitter generate another key K_D, and encrypt the data segment composed by original data and the new feature code C_F after encryption: $encode(data + C_F, K_D) \to Q$. That will be used to ensure the confidentiality of data during network transmission.

***Step 4*:** Use the public key of receiver PK_u to encrypt K_D, and set the result behind Q to form the final transmission data: $Q + encode(K_D, PK_u) \to H$.

On the side of receiver:

Step 1: The user decrypt the received data and get K_D by using its private key SK_u: $decode(H - Q, SK_u) \to K_D$.

Step 2: Using K_D to decrypt Q and get the original data and the feature code after encryption: $decode(Q, K_D) \to data + C_F$.

Step 3: Decrypt C_F by the public key (PK_c) of transmitter. If it can be done, the data has been proved sending by the correct transmitter, otherwise, the received data may not be sent from the pronounced transmitter.

Step 4: The user may take the same irreversible encryption method to calculate the feature code of received data, and compare it with C_F which is got from step 2. If they are identical to each other, the received data has not been distorted during transmission; if not, there might have some changes in the received data.

5. Conclusion

Under the fast development of mobile internet and cloud computing technology, location-based services have already become the new flashpoint and push factor in the mobile internet era. Facing with the increasing appearance of "Social + Local + Mobile" trends in the future, it is the best time to launch LBS system based on mobile cloud computing. However, privacy protection issue under mobile cloud computing environment is still the key factor influenced the further development of LBS services. The paper analyzed necessities and advantages to provide location-based services under mobile cloud computing environment; summarized traditinal methods to protect location privacy in LBS system; elaborated new security risks from the level of terminal, network and cloud platform; concluded the key points of

security needs for LBS system based on mobile cloud computing. Based on these works, the paper proposed a framework for cloud-based LBS system, descriped detailed implementation process of location-based services, and put forward privacy protection methods both for the outsourced LBS data and user information.

ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China (NO. 61363078, NO. 61265003), Natural Science Foundation of Gansu Province (NO. 1310RJYA004), and HongLiu Programme of Lanzhou University of Technology.

References

[1] Yin Jiwang. Development Status and Trend of LBS in the Era of Mobile Internet. China Internet. 2013; (6): 9-12.
[2] AT&T to launch cloud-based LBS mobility data offering, http://www.mobilecommercedaily.com/att-to-launch-cloud-based-lbs-mobility-data-offering
[3] http://network.51cto.com/art/201112/307344.htm
[4] http://lbsyun.baidu.com
[5] http://www.tomtom.com/en_gb/licensing/products/location-based-services/lbs-platform/
[6] Jiehui Ju, Jiyi Wu, Jianqing Fu, et al. A survey on cloud storage. *Journal of Computers*. 2011; 6(8): 1764-1771.
[7] Bingyi Fang, Yunyong Zhang, Jun Wu. Analysis on mobile internet application security issues based on the cloud computing mode. *Telecommunications Science*. 2013; 29(3): 41-47.
[8] Feng Xiao, Yajian Zhou, Jingxian Zhou, et al. Security Protocol for RFID System Conforming to EPC-C1G2 Standard. *Journal of Computers*. 2013 ; 8(3): 605-612.
[9] Man accused of stalking ex-girlfriend with GPS. http://www.foxnews.com/story/2004/09/04
[10] Sciannamea M. Companies increasingly use GPS-enable cell phones to track employees. http://wifi.weblogsine.com/2004/09/24
[11] Jia Jin-ying，Zhang Feng-li. Overview of location privacy protection technology. *Application Research of Computers*. 2013; 30(3): 641-646.
[12] Man Lung Yiu, Christian S. Jensen, Xuegang Huang, Hua Lu. SpaceTwist: managing the trade-offs among location privacy, query performance, and query accuracy in mobile services. *ICDE*. 2008; 366-375.
[13] Mokbel MF, Chow CY, Aref WG. Casper: query processing for location services without compromising privacy [J]. ACM Trans on Database Systems. 2009; 34(4): 24-48.
[14] Gruteser M, Grunwald D. *Anonymous usage of location-based services through spatial and temporal cloaking*. Proceedings of the 1st international conference on Mobile systems, applications and services. 2003: 31-42.
[15] Kar Way Tan, Yimin Lin, Kyriakos Mouratidis. *Spatial cloaking revisited: distinguishing information leakage from anonymity*. Proceedings of the 11th International Symposium on Advances in Spatial and Temporal Databases, 2009; 117-134.
[16] To Quoc Cuong, Dang Tran Khanh, Küng Josef. A Hilbert-based framework for preserving privacy in location-based services. *International Journal of Intelligent Information and Database Systems*. 2013; 7(2): 113-134.
[17] Yang Chao-hui, Li Shan-ping, Lin Xin. Anonymity level adaptation algorithm to meet resource constraint of K'anonymity service in LBS. *Journal of Zhejiang University (Engineering Science)*. 2011; 7: 1154-1160.
[18] Xu T, Cai Y. Exploring historical location data for anonymity preservation in location-based services. *The 27th Conference on Computer Communications*. 2008: 1220-1228.
[19] Niu Ben, Zhu Xiaoyan, Chi Haotian. Pseudo-Location Updating System for Privacy-PreservingLocation-Based Services. *CHINA COMMUNICATIONS*. 2013; 10(9): 1-12.
[20] Niu, Ben; Zhu Xiaoyan, Chi, Haotian. 3PLUS: Privacy-Preserving Pseudo-Location Updating System inLocation-Based Services. *IEEE Wireless Communications and Networking Conference*. 2013: 4564-4569.
[21] Feng, Yunxia; Liu, Peng; Zhang, Jianhui. A Mobile Terminal Based Trajectory Preserving Strategy for Continuous Querying LBS Users. *The 8th IEEE International Conference on Distributed Computing in Sensor Systems*. 2012: 92-98.
[22] Gao Sheng, Ma, Jianfeng, Sun, Cong. Balancing trajectory privacy and data utility using a personalized anonymization model. *Journal of Network and Computer Applications*. 2014; 38: 125-134.

[23] Komishani, Elahe Ghasemi; Abadi, Mahdi. A Generalization-Based Approach for Personalized PrivacyPreservation in Trajectory Data Publishing. The 6th *International Symposium on Telecommunications (IST) with Emphasis on Information and Communication Technology*. 2012: 1129-1135.
[24] Lei, Po-Ruey; Peng, Wen-Chih; Su, Ing-Jiunn. Dummy-Based Schemes for Protecting Movement Trajectories. *Journal of Information Science and Engineering*. 2012; 28(2): 335-350.
[25] http://mi.itxinwen.com/2013/0315/477311.shtml
[26] Tiande Tong, Xudong Liu, Taofeng Guo, et al. Analysis and practice of cloud computing information security. *Telecommunications Science*. 2013; 29(2): 135-141.
[27] John Bethencourt, Amit Sahai, Brent Waters. *Ciphertext-policy attribute-based encryption*. Proceedings of the 2007 IEEE Symposium on Security and Privacy. Washinton, DC: IEEE Computer Society. 2007: 321-334.