International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
www.ijais.org

Cloud based Spatial Cloaking for Mobile User Privacy Preservation

Revathy Gangadaren M
Department of Computer Science and Engineering, MES College of Engineering
Kuttippuram, Kerala, India

Lijo V. P.
Department of Computer Science and Engineering, MES College of Engineering
Kuttippuram, Kerala, India

ABSTRACT

Mobile Cloud Computing has invoked a new era of mobile world. The rapid growth of the mobile cloud computing has given rises to many new security issues. The well known spatial cloaking technique based on k-anonymity concept is using in mobile devices for privacy preserved location based services. To avoid the difficulties of the cloaked region management in mobile device, existing device based spatial cloaking is transferred to cloud based spatial cloaking. It is ensure more involvement of the cloud to reduce the burden of mobile device.

GENERAL TERMS

Mobile Cloud Computing, Location Based Services, Spatial Cloaking

1. INTRODUCTION

The Cloud computing [1] will have major impact on the mobile world and apart from a usual calling device, user expect the mobile phone as personal information processing tool even as mobile servers. Mobile Cloud Computing (MCC) [2] or cloud computing for mobile world [3] is a booming technology for future mobile applications. MCC [2] can be defined as a combination of mobile web and cloud computing, where the data storage and processing will happen outside of the mobile devices. So the mobile devices do not need to be a powerful device since all the computing tasks are transferred and processed in the cloud servers. The mobile phones offer advanced services such as web browsing, instant message, web camera, connectivity options, [4] etc., even it can be act as mobile servers, so the security is becoming more and more important. The computing power and memory capability of mobile phones are hard to completely meet the requirements of running resource intensive services. So the importance of mobile security is getting increased.

The security related issues are of two types [2] [5]: the security for mobile users and the security for data. The mobile devices are exposed to numerous security threats and also have privacy issues for users. Although both the mobile users and the application developers benefit from storing large amount of data on the cloud servers than in the local systems, should be careful of dealing with the integrity, authentication and digital rights of stored data. There are two types of security systems are provided, device based systems and cloud based systems [6]. In the device based security systems, run the security system inside the device i.e., it is a resource consuming process. In MCC, this is not preferable. The basic idea of the cloud based mobile security is that, the security systems are run in the cloud for ensuring security of the device. The resources inside the mobile phones are usually scarce. So the resource usages of the mobile phones are very critical. The importance of cloud based mobile security is investigated by analyzing different techniques. The most popular types are cloudAV (in-cloud Antivirus) [7], cloud based SIM (Subscriber Identity Module) DRM (Digital Rights Management) [8], implicit authentication [9] [10], cloud based intrusion detection and response system [11], cloud based privacy [12], etc. The core idea of the system is to run the security systems in the cloud servers and run light weight process in the mobile device. Out of these different techniques, privacy preservation is an important issue both in terms of legal compliance and legal trust. The most popular privacy breaches are reported while using the location based services in the mobile devices.

Location based services (LBS) [12] has become a popular mobile services due to the wide use of GPS (Global Positioning System), RFID (Radio Frequency Identification), etc. In order to entertain LBS, users need to provide exact location information to the services provider. Privacy concern arises if the intruders can configure out who issues the LBS request or where the request issuer is. The LBS faces a privacy issue when the mobile users provide private location information and other important information.

The remainder of the paper is organized as follows. The section 2 describes the survey on different cloaking techniques. The section 3 gives the observation and analysis based on the survey and the section 4 proposed a solution for enhancement. And also a conclusion and future work is made.

2. LITERATURE SURVEY

With the booming trends of positioning techniques, social computing [13] and the wireless short range techniques, the many of mobile users are using location based services. The LBS faces privacy issue when mobile users provide private information such as location, identity information, etc. With the widespread use of location services and social services in mobile devices and recent advances in location tracking technologies, the severity to numerous privacy threats are getting increasing. With untrustworthy LBS providers, the revealed private identity or location information could be misused by intruders.

Privacy-preserving techniques [12] are mainly based on any of the three concepts. (a) Dummies. Users protect their location privacy by reporting their exact locations with a set of fake locations, termed dummies, to a location based server.

It cannot provide high quality services due to the large amount of fake information. (b) Space transformation. The user location information and data are transformed into another space in which their exact or approximate spatial relationships are maintained to answer location-based queries. But it reveals the exact location to the issuer. (c) Cloaking. The main idea of the cloaking technique is to blur a user's exact location into a cloaked area that satisfies the user's privacy requirements, K-anonymity and minimum area. It provides aggregate location information to the server and gives better privacy than the other two techniques.

In terms of architecture models, existing spatial cloaking techniques can be categorized into three models, centralized, distributed and peer-to-peer. For the centralized architecture model, a trusted third party, termed location trusted server (LTS) is placed between the end user and the location-based service provider. The LTS is responsible for blurring users' exact locations into cloaked areas. This architecture model could pose a scalability issue because it requires all the mobile users to periodically report their exact locations to the LTS. Also, storing the user's exact location at a central server could pose a privacy breach. For the distributed architecture model, the users maintain a complex data structure to make the cloaked region through fixed communication infrastructure. But this model cannot be applied to highly dynamic location based mobile applications. For the peer-to-peer model, mobile users are work together to make cloaked areas at client side without using any fixed communication infrastructure or centralized/distributed servers.

2.1 P2P k-anonymity Model

The P2P k-anonymity model [14] is the Universal model proposed by Chi Yin Chow et al. This model constitutes the initial peer and other k-1 mobile peers to a group of k users to achieve the privacy with two important requirements: k and Amin, where k is the indistinguishable degree for the group and Amin is the minimum resolution of the cloaked area. In this model the k-anonymity is preserved i.e., the initiator cannot be distinguished from other k-1 peers. The P2P k-anonymity algorithm has several steps: 1) Select a central peer as an agent. 2) The agent will discover other k-1 different peers via single-hop or multi-hop to compose the group of k users. 3) Find a cloaked region with group of k users, covering all locations that every peer may arrive. 4) Adjust the cloaked region. Once the cloaked region is less than Amin, the region will be expanded.

This model achieves the user's privacy effectively. But the P2P k-anonymity algorithm builds on a strong inner trust and only considers the anonymity to server. But sometimes a collaborator may be present in the group. Another problem of this model is the variable network topology which brings a high disconnect rate and brings down the systems availability since it cannot be applied to highly dynamic mobile applications.

2.2 Mobile-aware Cloaking Model

The non-central and self organization architecture, called anonymous architecture is used in this model. In this architecture [14], all peers are anonymous peers. Anonymous peers are the peers have no information except from whom a query is received and to whom the query will be forwarded, so it has no knowledge of the initiator and the final receiver. In anonymous architecture, also need to achieve the k-anonymity and Amin.

The mobile aware algorithm for anonymous architecture consists of three phases [14]: Peers Discovering, Mobile-aware selection and Adjustment. In phase1, the initiator will broadcast a 'hello message' to its one hop or multi hop neighbors to discover new peers and add those new peers in a set T. In Phase 2, calculate the disconnect probability of two moving peers, i.e., $S = r / D$ where r is the transmission range and D is the distance between two peers and then the strongest connection peers are selected as next peer. If the discovered peers are not up to k, expand the peer set. In Phase 3, area covering all peers is computed and k value is checked. Phase 1 and Phase2 will be repeated until k peers and minimum area covering the peers are satisfied.

The mobile-aware algorithm improves the system connectivity remarkably by considering the mobility and selecting a relatively stable peer as its next hop.

2.3 Resource-aware Cloaking Model

The in-network resource-aware location anonymization algorithm is established [15] for wireless sensor networks. In this system, each sensor node blurs its sensing area into a cloaked area, in which the k-anonymity has to be preserved.

The location anonymization algorithm has three phases [15]. In phase 1, the objective of broadcast step is to ensure that each sensor node knows an adequate number of objects i.e., at least k objects to compute a cloaked area. Initially each sensor node m has an empty peer list. The node m send a message (identity: m.id, sensing area: m.area, number of objects in this area m.count) to its neighbors. When the node receives this message, it stores the message in peer list and check against the adequate number of objects. If node m finds adequate number of objects, it sends a notification message. If m has not received notification messages from all of its neighbors, then m forward the received message. This step reduces communication cost, because it relies on a heuristic that a sensor node only forwards its received messages to its neighbors when some of them have not yet found an adequate number of objects. In phase 2, the cloaked area step, to preserve the privacy requirements and to minimize the computation cost each sensor node blurs its sensing area into a cloaked area by using a greedy approach based on the information stored in peer list. For each sensor node m, calculates a score for each peer in its peer list. The score is defined as a ratio of the object count of the peer to the Euclidean distance between the peer and m. Based on these calculated scores, select a set of peers from peer list to form a cloaked area that includes at least k objects and has an area as small as possible. Then it repeatedly selects the peer with the highest score from the peer list to S until S contains at least k objects. Finally, m determines the cloaked area that is a minimum bounding rectangle (MBR). MBR is a rectangle with the minimum area that completely contains all desired regions. In phase 3, the validation step is to avoid reporting aggregate locations with a containment relationship to the server. If the two region's monitored areas are overlapping then it pose privacy leakage, is called containment relationship.

Each sensor node reports only aggregate location information to the server with the privacy requirements k-anonymity and Amin. The value of k achieves a trade-off between the privacy protection and the quality of monitoring services. The resource aware algorithm ensures that each sensor node finds adequate number of persons and uses greedy approach to find

cloaked area thus it aims to minimize communication and computation cost.

2.4 Quality-aware Cloaking Model

The quality-aware algorithm [15] aims to minimize the size of the cloaked area in order to maximize the accuracy of the aggregate locations. This model takes the cloaked area computed by the resource-aware algorithm as an initial solution, and then refines it until the cloaked area reaches the minimal possible area, which still satisfies the k-anonymity privacy requirement. The quality-aware algorithm initializes a variable current minimal cloaked area by the input initial solution by the resource-aware algorithm and it ends with the current minimal cloaked area contains the set of sensor nodes that constitutes the minimal cloaked area.

In general, the algorithm has three steps. In the search space step, the search space has to be determined. The typical sensor network has a large number of sensor nodes; it is too costly to collect the information of all the sensor nodes to compute its minimal cloaked area. To reduce communication and computational cost, sensor node determines a search space, based on the input initial solution, such that the sensor nodes outside of the search space cannot be part of the minimal cloaked area. To determine search space has two steps. (1) Find the minimum bounding rectangle (MBR) of the sensing area of A. (2) For each edge of the MBR, compute an MBR by extending the opposite edges In the next step, the minimal cloaked area step, takes a set of peers residing in the search space, as input and computes the minimal cloaked area. In this phase, needs to search all the possible combinations of these peers, so it could be very costly. Thus use two optimization techniques to reduce computational cost. In the first technique do not need to examine all the combinations of the peers in S; instead, only need to consider the combinations of at most four peers. The second optimization technique is progressive refinement and has two properties, lattice structure and monotonic property. In the last step, the validation step is to avoid reporting aggregate locations with a containment relationship to the server.

2.5 Casper Cloaking Model

Casper cloaking [16] is based on the bottom up generation method and it works on the statistics of the user locations. It employed a grid structure that hierarchically decomposes the whole space into levels. The root of the grid is at the level zero that covers the whole space and has only one grid cell. The Casper cloaking algorithm first locates the request issuer in a corresponding grid cell and checks the number of users in the grid cell. If it satisfies the k-anonymity then the grid cell as the cloaking region. If not it checks for the horizontal or vertical cells and check the total number of users in cell plus horizontal cell or cell plus vertical cell. The horizontal sum is checked against the vertical sum, if the greatest sum is greater than k, and then selects it as the cloaked region. The above check is not meet the k-anonymity goes up the parent grid.

Casper cloaking works well in the traditional architecture model because it can generate the smallest possible cloaked region safely and quickly and it provides good quality of services.

2.6 In-Device Spatial Cloaking Model

A simple approach for in-device cloaking [16] is to keep the grid structure inside the mobile device and do cloaking on the client side i.e., mobile devices are responsible for generating the cloaked area. In this model mobile client indexes a grid structure which partitions the space recursively. For each grid cell, collect the number of users from the cloud at a given time. The cloud will keep all updated user locations. As mobile users are moving constantly, the total number of users inside grid cells is changing over time. Once a client generated a cloaked region, device send the cloaked region as part of the request to LBS with identity information appropriately removed. The key is that we do not reveal that the issuer is in a cell before we are sure that the number of users in the cell is kept the k-anonymity concept.

This cloaking algorithm always works on a current node, which is set as the root of the grid. It then asks for the live numbers of users in its four child grid cells from the cloud servers. If the child cell c containing the request issuer does not meet the k-anonymity, it will check the sum of live number of users in c and in the horizontal neighbor or vertical neighbor. If this sum is no less than k, return the region as the union of grid cell c and the neighbor which has live number of users no greater than k and also require that the live number of users in horizontal or vertical be less than k as well. When the bottom level of the grid is reached, it stops by returning the bottom cell containing the issuer. There two optimization techniques to this model. 1) Instead of asking the live number of users for the grid cells, can ask for a sub tree of certain depth, then the communication overhead can be reduced. 2) To avoid starting from root node, use the upper and lower bounds to guide when to communicate with the cloud and when to go lower levels. This method maintains low communication cost with good quality of service.

2.7 Dual-active Spatial Cloaking Model

In the dual active mode design [17], instead of passively searching other peers for location information, the mobile clients can actively send their own locations as well as broadcast their gathered locations to other peers. The candidate peer location is defined by a 5-tuple record (uid, x, y, hop, initial Time), where uid indicates the user's unique identifier, x and y indicate the user's exact location, hop implies the distance between two peers and the initial time determines the time when the record is firstly broadcasted by the owner.

The dual-active algorithm is composed of four phases [17]. These are broadcasting, receiving, updating and querying phases. The mobile devices are automatically execute the broadcasting phase in the background periodically. Then the user begins to send own location record and also send all the records from his candidate peer list with the hop value increased by one. In the receiving phase, the user receives record from his direct neighbors. When the users are densely located, many redundant records are received. So the user filter redundant records based on hop and initial time values. The updating phase is executed to calculate the mean time between the current system time and the initial time of each record. If this mean time is larger than the pre-defined maximum time, it implies that these records have expired and should be removed by the user. In the querying phase, when launching a query, user can immediately begin the location cloaking calculation if the number of the candidate peers satisfies k-anonymity requirement. If the anonymities are not enough or the cloaked region does not fit for the privacy requirements then the mode enables user to recheck the situation periodically.

3. OBSERVATION AND ANALYSIS

The survey infers that, the drawbacks of the traditional cloaking techniques are getting improved by using different types of enhancements. In the mobile-aware cloaking techniques the privacy and connectivity are getting improved. In the case of resource-aware cloaking, it aims to minimize the communication and computational cost, while the quality-aware algorithm aims to minimize the size of the cloaked areas in order to generate more accurate aggregate locations. In-device cloaking device will be advantageous in many situations; it aims to provide safer cloaking with minimized communication cost. The dual-active approach uses the least anonymizing time and the best anonymization success rate at the expense of acceptable communication cost.

While using the location based services, privacy preservation by spatial cloaking is very important tack. In the case of centralized architectural models this task is done by the LTS and in the distributed one, it is done by base stations or fixed infrastructure. In the peer to peer architecture, the cloaking task is done by the mobile devices itself. When considering the MCC environment, it is a tedious task for thin mobile clients and has to keep the grid structure up to date within the device. So there should be a measure to reduce this burden on thin client to ensure more involvement of cloud. Now a day, the mobile devices are responsible for creating spatial cloaking regions and send this region to the location based server. It provides better privacy protection but it need to keep the grid structure up to date within the device. In MCC, the mobile phones are assumed to be thin clients, i.e., resource less devices, and all the processing wants be transfer from client side to cloud side. So this cloaking management is a difficult task for thin clients, has to be transfer from device to cloud.

4. PROPOSED SYSTEM

A mobile user wants to access the range queries like “nearest hospital”, “nearest ATM” etc., from the location based server. With untrustworthy servers, the location based services may lead to major privacy threats. In the proposed solution, a mobile user initiates an encrypted location based request to the cloud. The cloud employed a grid structure for the entire space. Then cloud indexes all updated user locations. The cloud has a large number of distributed virtual servers. The immediate server receives the encrypted request from mobile clients. According to the geographical location of the mobile device, the request is forwarded to the corresponding location based servers. Before sending request to the LBS, cloaking is done by the cloud servers.

The cloaking algorithm is run by the cloud servers. For each grid cell, check the number of users at a given time. Based on the k-anonymity concept the cloaking is done in the cloud. The cloaked area with the query is send to the LBS. The request from the mobile device is transferred to the cloud servers. If the immediate cloud server is busy then the request is transferred to the other servers. The answer set from the LBS is send back to the cloud servers and then back to the mobile device by using the session id. The answer can retrieve from the nearest cloud server. The cloud server lists the location based services in the specified region. The architecture is shown in Figure 1.

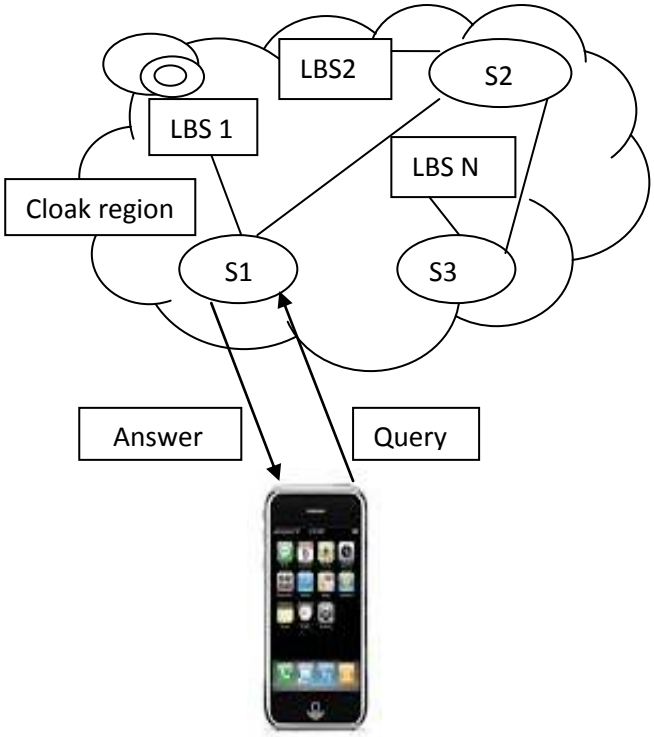

Figure 1 : Cloud Based Cloaking

The mobile device sends a query to the cloud server S1, call it as immediate server. Large numbers of location based services are provided by the service providers. These services can be accessed by the cloud. The cloud servers are responsible for the cloaking and these region plus query are sending to the untrustworthy service providers.

4.1 System Design

The proposed system mainly consists of three modules 1) Location Based service provider 2) Cloud servers with load balancing and cloaking algorithms 3) Thin mobile device with encryption and filtering algorithms.

The service provider has to update their service information. The cloud has to keep the updated services of the service providers. If N servers are available, then load balancing between the locations based servers has to be encountered. If LBS1 is busy then the query is implicitly forwarded to the LBS 2 etc. i.e., in general the end user can access the services of LBS 1 from LBS 1,2,…N. When considering the location based services, it can classify as proximity services, rescue services, hotel information, browsing, etc. The cloaking and load balancing must be performed by the cloud servers. The device has to be run light weight process as a proxy server for accessing services.

4.2 Advantages

The direct communication between mobile client and the untrustworthy service provider is not needed. So the privacy getting improved. The communication delay can be reduced by replacing the peer search through mobiles by user density information from cloud. Filtering in the mobile device for the exact answer set is not needed. Free the mobile device from the cloaking then the resource utilization is improved. The updated grid structure is not maintained in the device itself.

The most of the existing algorithms are build on a strong inner trust between the mobile devices and only consider the anonymity to the service provider. But there is a big chance for intruders may be in the group. The proposed system is a remedy for this attack.

5. CONCLUSION AND FUTURE WORK

With the rapid growth of mobile devices and the huge shift from the mobile as a calling device to mobile as a computer or server in future, the importance of mobile cloud computing is day by day getting increased. In the mobile cloud computing environment, the importance of privacy is identified. The different techniques for preserving privacy, while dealing with location based services are analyzed. The proposed method, the cloud based spatial cloaking is an enhancement to the existing cloaking methods.

For improved privacy, different levels of cloaking are suggested for the future work. First level cloaking is performed at client side and then second level cloaking at the server side or preferably different levels at the server side itself.

6. REFERENCES

[1] Wei-Tek Tsai, Qihong Shao, Xin Sun, Jay Elston, "Real-Time Service-Oriented Cloud Computing", in proceedings of the IEEE 6th World Conference on Services, 2010.

[2] H. Dinh, C. Lee, D.Niyato, and P. Wang, " A survey of mobile cloud computing: architecture, applications, and approaches", Wiley Online.

[3] Chetan S, Gautham Kumar5, Dinesh, Mathew K, and Abhimanyu M.A., "Cloud Computing for Mobile World", journal available at chetan.ueuo.com, 2010.

[4] M.La Polla, F. Martinelli, D. Sgandurra, "A Survey on Security for Mobile Devices", in proceedings of the IEEE Communications Surveys & Tutorials, 2012.

[5] S. Srinivasamurthy, and D.Liu, "Survey on Cloud Computing Security", Indiana University, 2010.

[6] X. Lin., "Survey on cloud based mobile security and a new framework for improvement," in proceedings of IEEE International Conference on Information and Automation (ICIA), 2011, pp. 710-715.

[7] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, "Virtualized in-cloud security services for mobile devices," in Proceedings of the First Workshop on Virtualization in Mobile Computing, ACM, 2008, pp.31-35.

[8] P. Zou, C. Wang, Z. Liu, J. Wang, and J. Sun, "A cloud based sim drm scheme for the mobile internet," in Proceedings of the 17th ACM conference on Computer and communications security, ACM, 2010, pp. 759-761.

[9] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices," in Proceedings of the 4th USENIX conference on Hot topics in security, USENIX Association, 2009.

[10] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, "Authentication in the clouds: a framework and its application to mobile users," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop, ACM, 2010, pp. 1-6.

[11] A. Houmansadr, S. Zonouz, and R. Berthier, "A cloud-based intrusion detection and response system for mobile phones," in Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops. IEEE Computer Society, 2011.

[12] C.Y.Chow, M.Mokbel, andX. Liu, "Spatial cloaking for anonymous location-based services in mobile peer to peer environments", GeoInformatica, Springer,2011.

[13] V.D. Dhale, and AR Mahajan, "Review of Cloud Computing Architecture for Social Computing" IJCA Proceedings on National Conference on Innovative Paradigms in Engineering and Technology (NCIPET), 2012.

[14] J.Xu, Jin, M. Zheng, "Mobile-Aware Anonymous Peer Selecting Algorithm for Enhancing Privacy and Connectivity in Location-Based Service", in Proceedings of the IEEE 7th Conference on e-Business Engineering, 2010.

[15] C.Y.Chow, M.F. Mokbel, and T. He,"A privacy preserving location monitoring system for wireless sensor networks", IEEE Transactions on Mobile Computing, 2011.

[16] S.Wang, and X. Wang, "In-device spatial cloaking for mobile user privacy assisted by the cloud", in Proceedings of the 11th IEEE International Conference on Mobile Data Management (MDM), 2010.

[17] Y.Che, Q.Yang, and X.Hong, "A dual-active spatial cloaking algorithm for location privacy preserving in mobile peer-to-peer networks", in Proceedings of the IEEE on Wireless Communications, 2012.