Quality Enhancement of Location Based Services Through Real Time Context Aware Obfuscation Using Crowd Sourcing

Priti Jagwani[1(✉)] and Saroj Kaushik[2]

[1] School of Information Technology, Indian Institute of Technology,
Hauz Khas, New Delhi 110016, India
jagwani.priti@gmail.com

[2] Department of Computer Science and Engineering,
Indian Institute of Technology, Hauz Khas, New Delhi 110016, India
saroj@cse.iitd.ac.in

Abstract. Widespread usage of Location based services (LBS) has eventually raised the concern for user's privacy. Various privacy preserving techniques are based on the idea of forwarding cloaking area to service provider who might be untrusted party, instead of actual location of query issuer/client. For such scenarios, in which cloaking area is exploited for privacy, results of the query request are generally based on nearest distance between client and service requested. Such techniques do not include real time context which is important in determining security, accessibility, etc. of the service and enhancing service quality. In this work, a novel method, based on crowd-sourcing concept has been proposed which takes into account the real time context for determining results of query. A system consisting of real time context-aware component is coined. Real time context has been obtained through crowd-resources available in cloaking area of client. A fuzzy inference system (FIS) has been proposed which takes nearest distance and real time context parameters as input. Based on these parameters FIS generates a new rank for the service requested. This rank is the new position on the answer list for the service requested. A prototype of the proposed system is implemented. Evaluation of prototype has been done by taking feedback of 112 users about their satisfaction in the range (0–10). User feedback for the prototype is compared with feedback of other similar systems using Kruskal Wallis test for significant differences. It has been discovered that user satisfaction for proposed system stochastically dominates other prevalent systems.

Keywords: Location based services · Security · Quality enhancement · Fuzzy inference system · Cloaking area

1 Introduction

Location Based Services (LBSs) are important and useful in almost all applications in mobile systems. Wide usage of smart mobile devices and advancement in positioning technologies have open up sky limiting possibilities in the domain of LBSs. The LBSs

O. Gervasi et al. (Eds.): ICCSA 2017, Part VI, LNCS 10409, pp. 79–94, 2017.
DOI: 10.1007/978-3-319-62407-5_6

are information services that provide users with required personalized contents, such as the nearest restaurants/hotels/clinics, which are retrieved from spatial databases. Potential LBSs applications can be countless ranging from Point of interest (POI) to complex navigation systems including proximity based marketing, fraud prevention, etc. These applications utilize the positioning capabilities of the device to determine the current location of the user. The location serves as an integral part of input for the location based services. The advantages of LBSs are very obvious and make life easier but they open up various vulnerabilities because of location knowledge. Location is often perceived as personal and sensitive information which can put a user's privacy in danger if mishandled by malicious actors. Thus, location disclosure can create threats to user's privacy. Recent research is being conducted on protecting location data [8, 11, 12, 23]. Approaches to safeguard location data can be based on policies and regulations, data transformations or location obfuscation.

Location obfuscation is a widely acknowledged category of location privacy mechanism in a ubiquitous computing environment. Obfuscation can be defined as deliberately degrading the quality of information in order to protect the privacy of the individual to whom that information refers. This process of degrading can be based on slightly altering, substituting or generalizing the location in order to avoid the real location of the user. A well focused technique of obfuscation is location cloaking in which exact location of user is blurred into a cloaked area based on some number K (K anonymity). After cloaking, a user is considered as K-anonymous if exact location of user cannot be distinguished among K-1 other users. The cloaked area contains at least K users including client. In a commonly used setting, client sends its service request to middleware which is actually a trusted party and is aware of user's location. The location of user can be determined using any of the available positioning techniques. Client gives query to service provider routed through middleware who generates clocking area around the client and sends it to location service provider (LSP). Assumption is that LSP may be considered as an untrusted party and hence should not know the actual location of user seeking service through him. Since a location service provider (LSP/Location Server) does not know the exact location of client thus providing client a security. LSP returns an answer set which are further filtered/arranged by middleware according to user's location. (Query and service request both refers to the request asked by client hence now onwards these terms can be used interchangeably).

These results of a service request are based on nearest distance method. Such methods lack in terms of inclusion of real time context. Results of such requests without inclusion of real time context may not be very effective for the client. For example, by getting a service or POI in the results which is not working presently, or is unreachable, etc. user may have a disappointing experience. To tackle such scenarios, real time context should be included with the results. Some context information can be collected through web also but here the requirement is of real time context for which the best sources are the human beings currently available at that place commonly known as crowd resources. Thus collection of real time context is based on crowdsourcing application model where crowd resources are used.

According to Jeff Howe crowdsourcing refers to a distributed problem-solving model in which a crowd of undefined size is engaged to solve a complex problem through an open call. Crowdsourcing is also defined as the act in which a company or institution take a task and outsource it to an undefined network of people in the form of an open call [1]. The task solving by distributed large group of people, who belongs to different disciplines is an example of crowdsourcing approach. An organization identifies tasks and releases those tasks online to a crowd of outsiders who are interested in performing these tasks on behalf the organization for a stipulated fee or any other incentives. A vast number of individuals then offer to undertake the tasks individually or in a collaborative way. Researchers have investigated the opportunities of using crowdsourcing for mobile applications thus making use of the real world context. Overall crowdsourcing system has emerged as a new problem-solving paradigm [2].

A novel location obfuscation system is proposed in the paper to include real time context, referred as real time context-aware obfuscation system. The system works for determining results of a service request within a cloaking area. The paper sets out a formal system, in which not only obfuscation of location-based services for the purpose of security is implemented but service quality is enhanced by inclusion of real time context. The proposed system is a generic LBS system and point of interest (POI) query has been taken as an example service so henceforth discussion presented will be with reference to the POI services.

Validation of proposed system is done by implementing prototypes for the proposed system and other two systems namely nearest distance method (most prevalent one) and security accessibility system. Security accessibility is the system in which rank of a POI is determined by its ranking of security and accessibility. For this system result set may contain candidate answers outside the cloaking area. Feedbacks for all the three systems have been collected by 112 users in terms of a score in the range (1–10). Feedback score given by the users are compared using Kruskal Wallis test. This test proved to be significant which indicates that feedback scores for the proposed system stochastically dominate the values of feedback score for other systems. The main contributions of this work are as follows:

- Inclusion of real time context component with well known obfuscation framework.
- Blending of real time context with the results of nearest distance method using FIS.
- Use of Kruskal Wallis test for the stochastic establishment of the proposed system has been explored. The test verifies the value of user feedback for proposed and some prevalent systems for significant differences.

Remainder of this paper is organized as follows. Section 2 presents related work along with necessary background. Overall system design is presented in Sect. 3, followed by Sect. 4 containing experimental settings, implementation and performance analysis. Section 5 contains statistical establishment of the system while conclusion and future directions are discussed in Sect. 6.

2 Related Work

Spatial *K*-anonymity paradigm has been widely studied in [3–6]. The client sends its *service request* to a trusted anonymizer, which constructs an anonymizing spatial region (ASR)/cloaking area that contains the location of client along with other (*K*-1) client locations. The anonymizer then sends the cloaking area to the LBS. The latter executes the service request with respect to the cloaking area, and returns a superset of the results to the anonymizer, which filters out the false positives.

Context aware computing offers the promise of considerable improvement in service quality. Context awareness is the ability of systems to adapt more readily to user needs, models, and goals. Context awareness of privacy protection mechanism is a prominent research area. Pingley et al. introduced a Context-Aware Privacy-preserving LBS system (CAP) [7]. They devised a mechanism for protecting location privacy and achieving LBS accuracy on the basis of context. Challenges of violation of location privacy based on (i) user's location information contained in the LBS query payload, and (ii) by inferring a user's geographical location based on its device's IP address were addressed.

Zhang et al. in [8] focused on context aware location privacy protection (CLPP) for location based social networks (LBSN) where the privacy requirements of users are not constant and isolated. They designed algorithms to evaluate whether the users' published geo-content meet the user's privacy requirement.

Pournajaf et al. examined the problem of spatial task assignment in crowd sensing when participants utilized spatial cloaking to obfuscate their locations [9]. They investigated methods for assigning sensing tasks to participants, efficiently managing location uncertainty and resource constraints. They proposed an optimization approach which consisted of global optimization using cloaked locations followed by a local optimization using participants' precise locations without breaching privacy. Interaction between application and crowd resources is being optimized for spatial task assignment along with addressing privacy concerns of users.

Damiani et al. coined probe framework for personalized cloaking of private locations which combines privacy personalization and location privacy [10]. The framework can be integrated with *K*-anonymity techniques and with policy-based approaches to provide stronger privacy protection especially in novel geosocial applications. They presented the idea to safeguard sensitive locations comprehensive of a privacy model and an algorithm for the computation of obfuscated locations.

Fawaz et al. proposed 'LP-Doctor', a light-weight user-level tool that allows Android users to effectively utilize the OS's location access controls while maintaining the required app's functionality [11].

Ju and Shin presented EMP2 tool for Location Privacy Protection for Smartphone users using Quadtree Entropy Maps. EMP2 accurately estimates the uncertainty of users' intended destinations and dynamically adjusts the protection level to defend against sophisticated inference attacks based on query correlation. Effectiveness of EMP2 has been demonstrated for effective protection of users' location privacy with reasonable computation time and resource consumption [12].

All the above research works were based on protection of location privacy using various versions of obfuscation techniques. In the past, researchers in different fields have used crowdsourcing concept. So far, the crowdsourcing work included Jana [13], a mobile crowdsourcing system, which publish simple tasks such as translation, transcription, and filling out surveys for mobile phones users. Google also uses crowdsourcing model to collect the road traffic data and provide the real time traffic conditions. Other location aware crowdsourcing services include mCrowd [17], and

GigWalk. mCrowd is a mobile crowdsourcing system in which micro sensing tasks are performed by crowd using their mobile devices. Gigwalk is a crowd-sourced service pays users for writing reviews and posting pictures. Some of other popular crowdsourcing systems are-Wikipedia, Yahoo! Suggestion Board, threadless, iStockphoto, InnoCentive, Sheep Market, Yahoo's flickr, MobiMission, Gopher game and CityExplorer, etc.

Crowd sourcing concept has been used in various research works. Erickson used geocentric crowdsourcing to enable cities and regions to more effectively address issues ranging from infrastructure to governance [14]. Liu et al. proposed location privacy recommender using user-user collaborative approach [15]. Yang et al. used Smartphone based crowdsourcing approach for indoor localization problem [16]. Nghiem et al. proposed a knn p2p query processing approach for mobile adhoc system [18]. They used the concept of data sharing from peers. Despite of lots of research about crowdsourcing model, usage of crowdsourcing in protection of location privacy and in enhancement of service quality is not fully explored yet. To et al. described idea to offer location privacy guarantees to crowdsourcing worker, based on differential privacy and geocasting [19]. They investigated analytical models and task assignment strategies that balance multiple crucial aspects of spatial crowdsourcing functionality, such as task completion rate, worker travel distance and system overhead.

Hu et al. employed peer to peer spatial *K* anonymity to protect worker's location privacy [20]. They also coined optimized schemes for spatial task assignment without compromising worker's location privacy. Toch presented a crowdsourcing framework for privacy management of location information in ubiquitous environment named 'Super-Ego' [21]. Crowdsourcing has been used to predict the user's privacy preferences for different location on the basis of the general user population.

Ubiquitous crowdsourcing is a little explored domain, in which the smart-phone users contribute information about their surrounding, thus providing a collective knowledge about the physical world. By applying ubiquitous crowdsourcing, the task of collecting information is performed continuously and in real-time. Mashhadi and Capra have explored the challenges for quality control in ubiquitous crowdsorucing and propose a technique that reasons on users mobility patterns and quality of their past contributions to estimate user's credibility [22]. In all the above works crowd resources are used in order to provide the service but in our work crowdsourcing is used to enhance the security and service quality of an already existing service by inclusion of real time context.

2.1 Problem Definition

In proposed work, the problem of service quality and security enhancement through inclusion of real time context obtained by crowdsourcing is explored. To explain the significance of inclusion of context in LBS, let us assume a scenario where, a user is asking for ATMs near his current location. Based on distance/geometry method, the user gets a list of 3 nearest ATMs; out of which the top/nearest two ATMs are not working or may be situated in isolated corners. The user may have a very embittered experience by these types of results. All these problems arise because the query results do not consider the just in time information, namely the security, accessibility, approachability and other elements of real time context while populating the reference space. Therefore those techniques are unable to provide user an upright service. So along with the protection of location privacy, need is for those techniques which are able to take into account the real time qualitative context in which users are located. For this the various parameters have been taken from crowd sources available at that place and these parameters are supplied as input to FIS. In this paper combination of server generated content (results of request generated by LSP) along with user-generated content (real time parameters) is being achieved using a fuzzy inference system (FIS). This is done in order to extend service quality of a task in the real world.

3 Overall System Design

This section presents the overall design and working flow of the proposed system. The system contains the following components: mobile client, middleware, crowd resources, location service provider (LSP). The middleware consist of various modules namely cloaking area generator module, real time context module, context based FIS module. Individual components of the proposed system are shown in Fig. 1 and described in detail in the following subsections.

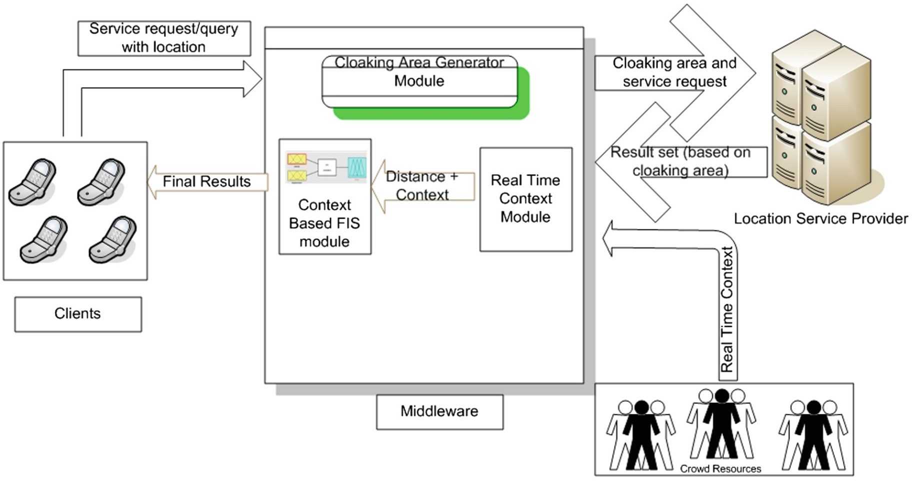

Service request/query with location
Cloaking Area Generator Module
Cloaking area and service request
Result set (based on cloaking area)
Location Service Provider
Final Results
Distance + Context
Context Based FIS module
Real Time Context Module
Real Time Context
Clients
Middleware
Crowd Resources

Fig. 1. Architecture of the proposed system

3.1 Mobile Client with Web Interface

Client is a mobile user who sends the service request about a particular service to middleware. Client is registered with the middleware. Current position of this registered user can be automatically obtained by GPS enabled device. Location of the client is known to middleware. Further, service request is given to middleware. Client does not want to reveal its location to the untrusted parties like location service provider (LSP) or Location server. In the proposed approach, after completion of service request, client gets the response to his service request based on real time context blended with nearest distance. Client can also see the rank of POI requested which shows the reachability, accessibility and security of the queried point/object.

3.2 Middleware

Middleware is the central and trusted entity which operates between client and LSP. In general scenarios a middleware takes the location and request of client. This location is obfuscated to maintain the privacy. Middleware comprises of 3 main modules. These are:

- Cloaking area generator module.
- Real time context module.
- Context based FIS module.

Cloaking Area Generator Module: Given exact location of the client, the module generates a cloaking area around that location. It is ensured that at least *K*-1 users must be present in that area apart from the user. Cloaking area will be generated enclosing those K-1 users and client. The value of *K* is determined by this module using the techniques available in literature [23]. Regular shaped cloaking regions can be circular or rectangular. It has been proved by research that circular cloaking regions incurs a higher processing cost [24]. So rectangular cloaking areas are preferable over circular. There can be a number of methods for generating the rectangular cloaking area like Hilbert curve, NNC (Nearest neighbor cloaking), etc. For the purpose of our experiments we have used nearest neighbor cloaking area method. In this method cloaking area is a minimum bounding box which encloses all *K* users. This cloaking area along with the service request is given to LSP.

Real Time Context Module: This module receives the parameters of real time context from crowd resources and result set obtained by LSP. Finally, it supplies rating of distance between service and client (nearest the distance, higher is the ranking); and aggregated values of real time context parameters (of POI) to context based FIS module.

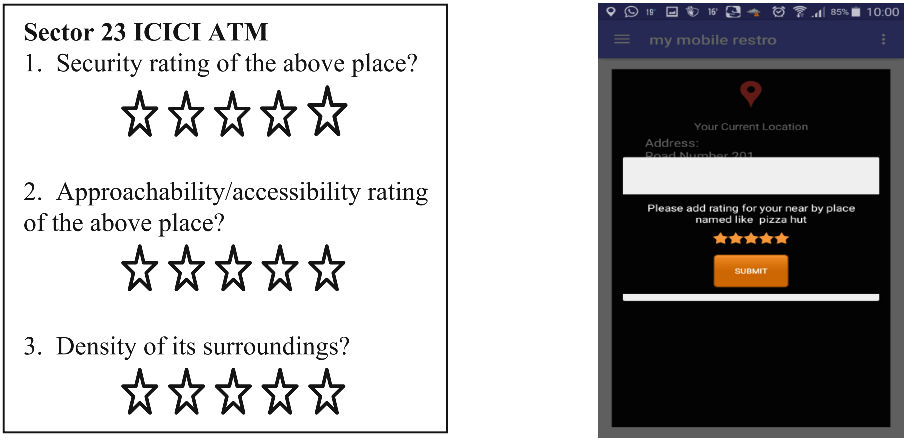
A set of environmental states and settings that are important in determining behavior of an application or service can be termed as Context. The proposed system deals with some specific elements of context namely security, and density of place, accessibility/reachability. Values of all these elements are in the range of 1–5 where 5 represents the highest and 1 represents the lowest.

Security of the location depicts the well-being of the place. In general scenarios, some places are considered less/more safe than others depending upon their sensitivity and well being. If one is unable to decide upon safety of a place using intuition/perception/already available information about the place, it can be easily obtained by many readily available applications. Example of one of such application is “safetypin” [www.safetypin.com].

Density of a place can easily be observed by users present in the area. It is an observation of footfall in that area. For the proposed system, another factor of context is reachability/approachability that basically determines how accessible/functional is the POI? Ratings of all these elements are asked from user present in the cloaking area through a predefined set of questions. These questions contains a rank/rating about.

- Security.
- Density of the nearby place.
- Accessibility/reachability of the POI.

Rating for all the above mentioned parameters is given by users/crowd resources present in the cloaking area. This rating is in the form of crisp numbers as shown in Fig. 2. Rating given by all users is aggregated/averaged for each element. Question interface is designed in such a way that these questions can be easily answered by the crowd resources within few clicks. Set of questions and sample interface is shown in the figure below.



Sector 23 ICICI ATM

1. Security rating of the above place?

☆☆☆☆☆

2. Approachability/accessibility rating of the above place?

☆☆☆☆☆

3. Density of its surroundings?

☆☆☆☆☆

my mobile restro

Your Current Location

Address:
Road Number 201

Please add rating for your near by place named like pizza hut

★★★★★

Fig. 2. Questions and sample interface

The request for rating is based on a timing constraint i.e. system waits for 20 s for rating after displaying the rating request on the crowd resource's mobile screen. Crowd resource has to provide feedback within 20 s. Real time context module stores this rating given by crowd resources for future use also.

The module also receives the result set from the LSP. The result set contains list of POIs in the cloaking area. These POIs are arranged in the increasing order of distance between client and POI/service. In this way, every POI is now having a rating corresponding to nearest distance also. Finally, ratings of distance, security, approachability and density are supplied to context based FIS module for further processing.

Context Based FIS Module: This module collects the rating of distance and real time context parameters from real time context module and after processing it generates new rank of POIs to be sent to the client.

The main component of context based FIS module is Fuzzy inference system. Fuzzy inference is the process of transforming a given input into required output using fuzzy logic. This process involves membership functions, fuzzy if then else rules and fuzzy operators. This module obtain the aggregated values of ratings of all real time context parameters and distance between client and requested POI, from real time context module. These parameters serve as input to FIS. Firstly, fuzzification of these input values takes place based on membership functions. Then fuzzy inference engine converts these inputs into output on the basis of rules. Based on the rules written in rule base, output value of FIS is determined which is the new rank of the POI. The whole process is shown in Fig. 3

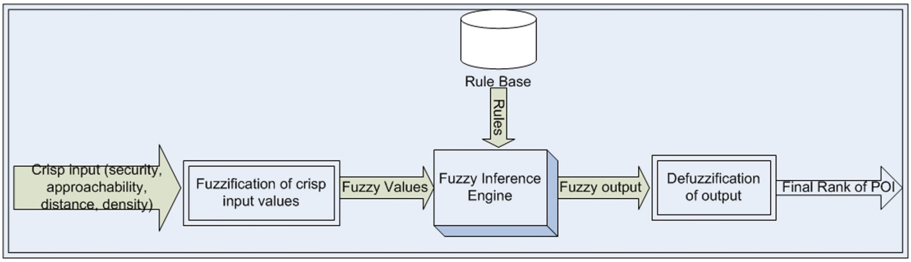

Rule Base
Rules
Crisp input (security, approachability, distance, density)
Fuzzification of crisp input values
Fuzzy Values
Fuzzy Inference Engine
Fuzzy output
Defuzzification of output
Final Rank of POI

Fig. 3. Fuzzy inference system

Around 350 rules have been coined intuitively based on different values of inputs and output. Some rules of FIS are shown below:

- If security/well being of the place is low, approachability/accessibility is very low, density is moderate and distance is far then rating is very low.
- If security/well being is moderate, approachability/accessibility is low, density is moderate and distance is near then rating is medium.

Output of this module is a new crisp rating of POI. In this way final ranked list of recommended POIs is obtained. This final list of POIs is sent to client as a result. Collectively, input values, processing done and output values of all the three modules of middleware are given in the table below (Table 1).

3.3 Location Service Provider (LSP)/Location Server

LSP is the service and content providing entity which is considered as untrusted. Some common examples of LSPs are Navteq, Tele Atlas, Google and many others. Location service provider offers a number of different services like finding a route or searching specific information on objects of user interest and many others. Typically, LSP

Table 1. Input, processing and output of various modules of middleware

Module name	Input	Input received from	Processing done	Output	Output given to
Cloaking area generator	Service request and client location	Client	Generation of cloaking area (CA)	Service request and cloaking area	LSP
Real time context	1. Real time context parameters 2. Service response with respect to CA	1. Crowd resources 2. LSP	Aggregation of each real time context parameter obtained by all users and determining Rating of POI according to nearest distance	Aggregated values of real time context parameters and nearest distance rating of POI	Context based FIS module
Context based FIS	Aggregated values of real time context parameters and nearest distance rating of POI	Real time context module	Fuzzy inferencing based on fuzzy rules	Final rank of POIs based on real time context and distance	Client

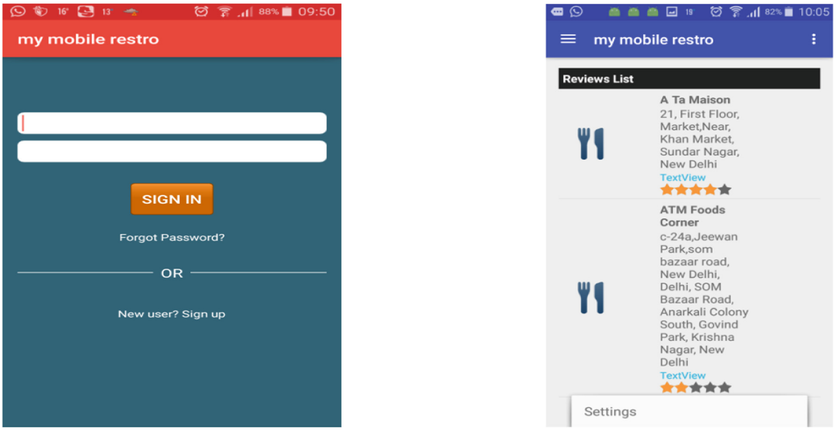
receives a cloaking area and service request from middleware. Then it returns the result set pertaining to that cloaking area to middleware.

4 Implementation and Experiments

In this section, we describe implementation details followed by experimental settings.

Implementation: In order to show the feasibility of the proposed system, prototype of the client side application and middleware are implemented. Middleware resides on server side while client side module is for the mobile handset of client. The whole application is developed using Android Software Development kit and PHP. For appropriate comparison of the system we have developed three prototype applications. One that returns the result solely on the basis of nearest distance (systems which are already prevalent, now onwards called as nearest distance method), another one which retrieves results on the basis of security and accessibility ranking only, and the third one (our proposed idea) which provides the result on the basis of combination of nearest distance and security-accessibility ranking. Some snapshots (login screen and rating generation snapshot) of the developed prototype are shown below in Fig. 4.

Experimental Settings: For assessment and evaluation of the proposed system we have taken crowd resources to work on it. These are volunteers registered in the system. There are total 112 such volunteers. Every volunteer install all the three systems on their smart phones and used them for three weeks. Volunteers provide a feedback score for all the prototypes. Their feedback given in terms of score about all



A Ta Maison
21, First Floor,
Market,Near,
Khan Market,
Sundar Nagar,
New Delhi

ATM Foods
Corner
c-24a,Jeewan
Park,som
bazaar road,
New Delhi,
Delhi, SOM
Bazaar Road,
Anarkali Colony
South, Govind
Park, Krishna
Nagar, New
Delhi

Fig. 4. Sample snapshots of prototype

the three systems have been taken and recorded for further analysis. This feedback is on a scale of (1–10) where 1 represents the lowest score (lowest satisfaction) and 10 represents the highest.

Table 2 represents the feedback given by volunteers for all the three systems. First column shows the score while other three columns represent number of users who have given the score displayed in the left most column for the respective systems. For example, 10.6% users have given score in the range of 1–3 to the nearest distance prototype while 24% users have given score as 4–6 to the same. This data is shown in the following graph also (Fig. 5).

Table 2. Feedback scores given by users

Score	Security accessibility prototype	Nearest distance prototype	Nearest distance + security accessibility prototype
1–3	19.6%	10.6%	5.3%
4–6	80.4%	24%	35.6%
7–8	0%	65.4%	32.0%
9–10	0%	0%	22.3%

From the given data in above table, one can easily interpret that for security accessibility prototype performs poor on satisfaction (0%) on higher score (7–10), nearest distance prototype performs good on satisfaction at level (7–8) but no user has given score between (9–10). The proposed system has overall higher satisfaction with minimum score of dissatisfaction (1–3), and with 22.3% of users have given score in the range (9–10). Further statistical evaluation of all the three systems is done by Kruskal Wallis test results which prove that data on which experiment is done is significant. Following section describe statistical test on the feedback values. Data presented in this section proves our claim that proposed system performs better in terms of satisfaction.

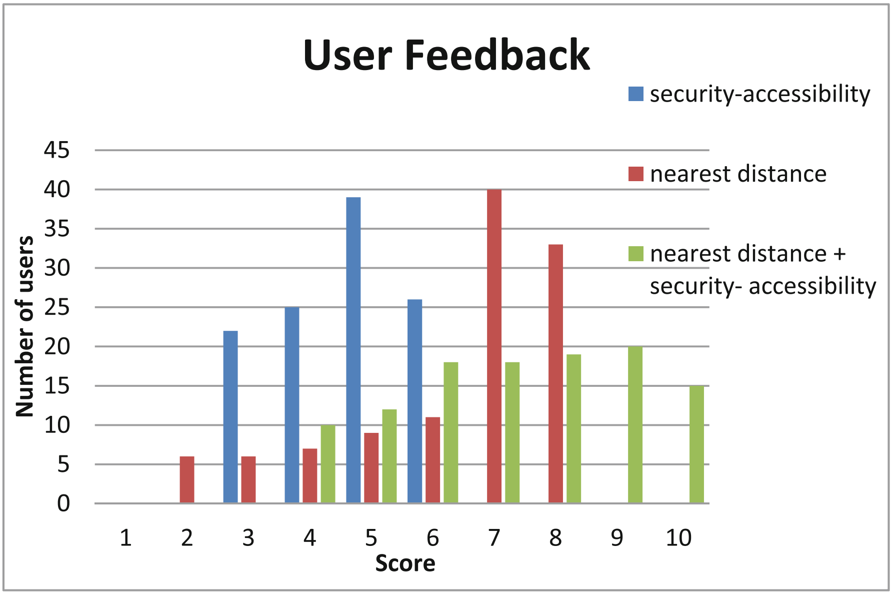


Fig. 5. Graphical representation of feedback scores

Performance Analysis: In the earlier subsection, performance of the proposed system has been evaluated in terms of feedback. The system has also been evaluated for response time as a metric. Results for response time taken as compared to the prevalent systems are shown in figure below.

Although the response time taken by our proposed system is greater than the prevalent system but this extra cost (in terms of time in sec) is paid in order to get real time security and current accessibility status. One may not want to go to an insecure place or an inaccessible/unapproachable, rather wants to invest some extra seconds in

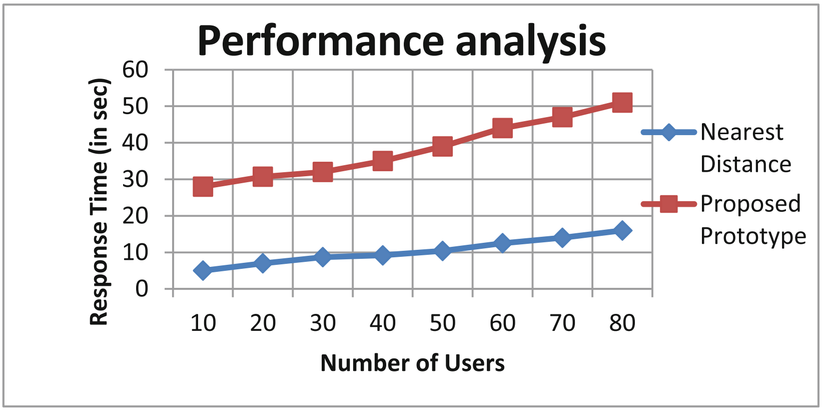


Fig. 6. Performance analysis in terms of response time

order to get actual real time status of POI. This fact has been proved by the better feedback given by users. This greater response time is because of an increased step of obtaining real time context from crowd resources and reranking the response on its basis. This step is not available in nearest distance method. Further, response time of a service is dependent on many design patterns like storage data structures, use of caching layers, archiving aging data to reduce table sizes, separate databases for read only and write only nodes, etc. Response time can certainly be improved by taking care of the above mentioned design patterns (Fig. 6).

5 Statistical Establishment of the System

In this section, for establishment of claims of proposed system, feedback values given by users are evaluated statistically. This evaluation is done to ascertain the fact that the difference between feedback values is significant and proposed system is performing better. For this Kruskal Wallis test has been applied on the feedback values. The Kruskal-Wallis H test (sometimes also called the "one-way ANOVA") is a nonparametric test that can be used to determine if there are statistically significant differences between the data samples. Also the Kruskal-Wallis H test does not assume normality in the data. That is why it is best suited for our data. Shown below are the results obtained from the kruskal's wallis test (with 5% significance level).

Here,

- var1 represents feedback ratings of the system with only distance as a metric
- var 2 represents the feedback of system with only security and accessibility as a metric
- var3 represents feedback of the system with distance and security-accessibility both as a metric.

Table 3 shows various summary statistics while Table 4 shows that there are significant differences between Var1 and Var3.

Table 3. Summary statistics

Variables	No. of observations	Observations with missing data	Observations without missing data	Min value	Max value	Mean	Std. deviation
Var1	10	3	7	6.00	40.0	16.0	14.3
Var2	10	6	4	22.0	39.0	28.0	7.5
Var3	10	0	10	1.00	18.0	11.2	6.2

Table 5 represents the null hypothesis and alternative hypothesis of the test performed and Table 6 contains sample mean scores, p value and significance level. Result interpretations are shown in Table 7.

Results clearly show that we can safely reject the null hypothesis which implies that the data is not drawn from the same population means the data is significantly distinct.

Table 4. Significant differences

	Var1	Var2	Var3
Var1		No	Yes
Var2	No		No
Var3	Yes	No	

Table 5. Test interpretation

H_0: The samples come from the same population. (Hypothesis)
H_a: The samples do not come from the same population. (Alternate Hypothesis)

Table 6. Results of Kruskal Wallis test

Sample mean score (Var 1)	4.616071429
Sample mean score (Var 2)	6.366071429
Sample mean score (Var 3)	6.598214
p-value (two-tailed)	0.0478
Alpha	0.05

Table 7. Results interpretation

As computed p-value is lower than the significance level alpha = 0.05, one should reject null hypothesis H_0, and accept the alternative hypothesis H_a
The risk to reject the null hypothesis H0 while it is true is lower than 4.78% (shown by p-value)
Also, highest sample mean score of feedback values for var 3 (proposed system) depicts outperformance the other systems

It is clear from the above results that there are significant differences between the var1 (feedback of the system with only distance as a metric) and var3 (feedback of the system with distance and security-accessibility both as a metric). Moreover, looking at the feedback ratings given by users, one can easily spot that proposed system has got higher scores of feedback. Highest sample mean score of feedback values for the proposed system depicts that our proposed system is performing better than the most prevalent nearest distance system.

6 Conclusions and Future Directions

In the work presented, a system has been proposed to enhance the security and accessibility of the location based services through inclusion of real time context. Experimental prototype of the proposed system is implemented by taking point of interest query as the example service. Crowdsourcing model has been used in obtaining the real time context which is collected from the crowd resources currently present in that area. Although a price is being paid in terms of increased response time (few seconds) but our system provides considerable satisfaction. Measures have been suggested to improve the response time. To evaluate the success of our prototype, feedback has been obtained from the users. Stochastic evaluation of the feedback showed that the proposed system outperforms the other prevalent systems.

The proposed system is in a prototype stage which can witness certain improvements in future. One can also device questions to be asked from crowd resources based on the service request type/content. Also to improve the service time, real time responses of previous queries (say of 15 min prior) can be saved in a separate database structure and the similar service request for the same area can be served on the basis of that stored data instead of asking crowd resources again. Moreover, credibility of crowd resources can be another area for improvement and further research based on which weightage to be given to the response of a particular crowd resource can be determined.

References

1. Howe, J.: Crowdsourcing: a definition, crowdsourcing: tracking the rise of the amateur. In: Crowdsourcing: Why the Power of the Crowd is Driving the Future of Business (2006)
2. Alt, F., et al.: Location-based crowdsourcing: extending crowdsourcing to the real world. In: Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries. ACM (2010)
3. Chow, C.-Y., Mokbel, M.F., Liu, X.: A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In: Proceedings of the 14th Annual ACM International Symposium on Advances in Geographic Information Systems. ACM (2006)
4. Kalnis, P., et al.: Preventing location-based identity inference in anonymous spatial queries. IEEE Trans. Knowl. Data Eng. **19**(12), 1719–1733 (2007)
5. Gedik, B., Liu, L.: Location privacy in mobile systems: a personalized anonymization model. In: 25th IEEE International Conference on Distributed Computing Systems (ICDCS 2005). IEEE (2005)
6. Yiu, M.L., et al.: Spacetwist: managing the trade-offs among location privacy, query performance, and query accuracy in mobile services. In: 2008 IEEE 24th International Conference on Data Engineering. IEEE (2008)
7. Pingley, A., et al.: CAP: a context-aware privacy protection system for location-based services. In: 29th IEEE International Conference on Distributed Computing Systems, ICDCS 2009. IEEE (2009)
8. Zhang, H., et al.: CLPP: context-aware location privacy protection for location-based social network. In: 2015 IEEE International Conference on Communications (ICC). IEEE (2015)
9. Pournajaf, L., et al.: Spatial task assignment for crowd sensing with cloaked locations. In: 2014 IEEE 15th International Conference on Mobile Data Management, vol. 1. IEEE (2014)
10. Damiani, M.L., Bertino, E., Silvestri, C.: The PROBE framework for the personalized cloaking of private locations. Trans. Data Priv. **3**(2), 123–148 (2010)
11. Fawaz, K., Feng, H., Shin, K.G.: Anatomization and protection of mobile apps' location privacy threats. In: 24th USENIX Security Symposium (USENIX Security 2015) (2015)
12. Ju, X., Shin, K.G.: Location privacy protection for smartphone users using quadtree entropy maps. J. Inf. Priv. Secur. **11**(2), 62–79 (2015)

13. Eagle, N.: txteagle: mobile crowdsourcing. In: Aykin, N. (ed.) IDGD 2009. LNCS, vol. 5623, pp. 447–456. Springer, Heidelberg (2009). doi:10.1007/978-3-642-02767-3_50
14. Erickson, T.: Some thoughts on a framework for crowdsourcing. In: Workshop on Crowdsourcing and Human Computation, pp. 1–4 (2011)
15. Liu, N.N., Zhao, M., Yang, Q.: Probabilistic latent preference analysis for collaborative filtering. In: Proceedings of the 18th ACM Conference on Information and Knowledge Management, CIKM 2009, pp. 759–766. ACM, New York (2009)
16. Yang, Z., Wu, C., Liu, Y.: Locating in fingerprint space: wireless indoor localization with little human intervention. In: Proceedings of the 18th Annual International Conference on Mobile Computing and Networking. ACM (2012)
17. Yan, T., et al.: mCrowd: a platform for mobile crowdsourcing. In: Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems. ACM (2009)
18. Nghiem, T.P., Waluyo, A.B., Taniar, D.: A pure peer-to-peer approach for kNN query processing in mobile ad hoc networks. Pers. Ubiquit. Comput. **17**(5), 973–985 (2013)
19. To, H., Ghinita, G., Shahabi, C.: A framework for protecting worker location privacy in spatial crowdsourcing. Proc. VLDB Endow. **7**(10), 919–930 (2014)
20. Hu, J., Huang, L., Li, L., Qi, M., Yang, W.: Protecting location privacy in spatial crowdsourcing. In: Cai, R., Chen, K., Hong, L., Yang, X., Zhang, R., Zou, L. (eds.) APWeb 2015. LNCS, vol. 9461, pp. 113–124. Springer, Cham (2015). doi:10.1007/978-3-319-28121-6_11
21. Toch, E.: Crowdsourcing privacy preferences in context-aware applications. Pers. Ubiquit. Comput. **18**(1), 129–141 (2014)
22. Mashhadi, A.J., Capra, L.: Quality control for real-time ubiquitous crowdsourcing. In: Proceedings of the 2nd international workshop on Ubiquitous Crowdsouring. ACM (2011)
23. Jagwani, P., Kaushik, S.: K anonymity based on fuzzy spatio-temporal context. In: 2014 IEEE 15th International Conference on Mobile Data Management, vol. 2. IEEE (2014)
24. Kalnis, P., Ghinita, G., Mouratidis, K., Papadias, D.: Preventing location-based identity inference in anonymous spatial queries. TKDE **19**(12), 1719–1733 (2007)