ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Protected Locality based Rewarding method Via Redemption System

Prerna Wankhede (Patil), Prof. Kodmelwar M.K

PG Student, Dept. of Computer Engineering, TSSM's BSCOER, Narhe, Pune, India

Assistant Professor, Dept. of Computer Engineering, TSSM's BSCOER, Narhe, Pune, India

ABSTRACT: Theoretical Location is rapidly transforming into the application as area empowered mobile handheld duplicate devices. One class of applications that has yet-to-create is those in which users have a force to lie about their location. These applications can't depend independently on the user's gadgets to discover and transmit location data in light of the way that users have a helper to swindle. Maybe, such applications require their users to show their locations. Today's mobiles clients neglect to offer a framework to show their current then again past location. In hate of the way that locations based applications have existed for a couple quite a while, affirming the rightness of a customer's declared locations is a test that has pretty much starting late got thought in the investigation bunch. Continued with advances in mobiles frameworks and arranging developments have made a strong business push for locations based applications. Cases fuse area mindful emergency response, locations based notification, and locations in light of entertained. A key test in the wide association of Location- Based Services (LBS) is the security careful organization of locations data. The late work in imparted media content what's more, sensed information made by versatile end-clients is trying settled gauges likewise assumptions in information trust models. A focal issue addresses in this paper is the way by which to fabricate some trust level in the realness of substance made by untrusted locations users. In this it handle the issue of discovering noxious users by putting away IMEI number while user registration. In this way framework saving security in compensating framework that implies redemption system. This number is encoded and put away in central controller. Token distributor and token collector are utilized for remunerating.

KEYWORDS: Mobile location-based services; security; privacy.

I. Introduction

As of late, there has been a ton of change in the number of area location administrations, with administrations like foursquare having incalculable users. A user location is a basic part for enabling these services. Various services rely on upon clients to successfully report their location. In paper [1], creator has proposed a protected, protection saving, and practical location based rewarding system, LocaWard. They have outlined a security and protection mindful protocol for the LocaWard framework and demonstrated its culmination and soundness. Lifelog [2], which has recreated authentic security concerns, confirm that reliably taking after where individuals go and what they do is not simply in the extent of today's inventive advances furthermore raises genuine individual protection issues, paying little personality to the various important applications that it can give.

As showed by the report by the Computer Science furthermore, Information moves Board in IT Roadmap to a Geospatial Future [3], location-based services (LBSs) are depended upon to structure a basic piece without limits registering circumstances that will be faultlessly and pervasively joined into our lives. Such services are starting now being made furthermore sent in the business and investigation planets. For instance, the Nextbus [4] organization gives location based transportation data. Web associations have utilized the benefits of open improvement and open APIs for a long time, yet portable heads are basically entering the open space with an thought alluded to here as Open Telco which explores how open APIs can be joined with mobile systems keeping in mind the final objective to change them from an uneven into two sided stage where new plans of activity can be utilized. The examination was started by making an arrangement of utilization circumstances for examination by a master gathering Above all, the Open Telco stage must back in any occasion national and in a perfect world, especially in portion circumstances, overall extension to extend the framework sways and to adjust to web contenders [5]. A huge security risk specific to LBS utilization is

DOI: 10.15680/ijircce.2015.0306086

the location security ruptures addresses by space or time connected incitement attacks. Such ruptures happen when a social affair that is not trusted becomes acquainted with information that reveals the location went to by the single person, and furthermore the times in the midst of which these visits happened. An adversary can utilize such area information to assemble experiences about the private existence of a single person, for instance, their political affiliations, elective lifestyles, or therapeutic issues [6] or the private organizations of a relationship, for instance, new business exercises and associations.

Location-based access control in the physical world is basic, standard, and ordinary. For example, having the limit to turn on or the lights in a particular room presupposes having vicinity in the room. The very blueprint of the light switch is the thing that actualizes the security game plan. Interestingly, fulfilling the same kind of protection with information structures, for example, remote frameworks, is less clear; it is not simply a matter of putting a switch in the benefit place. To engage location construct access control procedures with respect to information resources, framework oblige a way to deal with perform location confirmation, where an essential location is securely confirmed to meet certain criteria: e.g., being inside a particular room or a particular building. At the point when an essential location has been confirmed using a tradition for location confirmation, the essential can be surrendered access to a particular resource as showed by the wanted system. This approach is consistently merged with physical security; ensures or locks may be used to make sense of who is allowed to enter a building, then area check utilized to grant remote access to every one of those inside.

Along these lines, the location check issue is the key specific challenge that must be surmounted to complete location based access control. Location based access control has a couple advantages. One basic course of action may allow remote control of just the lights for the room you are in, or may request that an association server quit working if it is taken outside the building. Moreover, using location for access control is the need to make conferred special experiences ahead of time. Guests to a developing need not obtain remote encryption keys before their visit; rather, the keys could be yielded regularly to every single physical occupant of the building. In like way, at the baseball, fans at a ball game could get live scorecards on their remote devices, while stadium holders could confine this organization to simply those truly present in the stadium. It would be exceptionally massive to course new keys to all fans heading off to everyone redirection, yet area based get to control grants bootstrapping o the current physical security measures controlling section to the premises.

This paper is made further as: Section II discusses related work examined till now. Section III presents usage points of interest, calculation utilized and scientific model. Section IV closes with the conclusions and presents future work.

II. Related work

Prior take a shot at protection parts of telematics and location based applications has for the most part focused on a strategy based methodology [9]. Data subjects need to survey and pick security plans offered by the organization supplier. These techniques serve as a contractual seeing about which data can be accumulated, for what reason the data can be used, and how it can be spread. Frequently, the data subject needs to trust the organization supplier that private data is enough secured. On the other hand, the secrecy based methodology de-customizes data before gathering, in this way protection game plan and shields for data are definitely not separating. Yiu et al. propose an incremental nearest neighbour processing algorithm to retrieve query results [8]. The process starts with an anchor, a location different from that of the user and it proceeds until an accurate query result can be reported. The work focuses on reducing the communication cost of the repeated querying mechanism.

This requirement ensures that the user will not be uniquely located inside the region in a given period of time [10]. Ghinita et al. propose a decentralized architecture to construct an anonymous spatial region and eliminate the need for the centralized anonymizer. Mobile nodes in this method utilize a distributed protocol to self-organize into a faulttolerant network which is overlaid, from which a k-anonymous cloaking set of users will be generated. Kalnis et al. proposed all obfuscation methods needs to satisfy the property of reciprocity. That will prevent inversion attacks at which place knowledge of the underlying anonymizing algorithm can be used to identify the actual object. Parameter specification remains the biggest hindrance to real-world application of these techniques. Location protection has also been considered in position sensor structures. The Cricket structure [7] places location sensors on the mobile phone rather than the building structure. Thusly, location information is assuredly not uncovered the position determination process and the data subject can pick the get-togethers to which the information should to be transmitted. Location-sensitive applications require users to prove that they really are (or were) at the claimed locations. In many cases most mobile users have Smartphone devices which are capable of discovering their locations; some of the LBS using customers can cheat on their actual locations and which results in lack of secure mechanism to provide their current or past locations to applications and services [11].

WanyingLuo[12] present location evidence building plan that comprehends setup targets too that consolidates customer secrecy and location security as key design parts. In a presentation phase, the sender chooses a course through a plan of onion routers. The sender at that point again and again adds coordinating information to the payload and scrambles it using the onion routers public key. The outcome is an onion embodying a couple of layers of encryption that are peeled off while the packet goes through the switch. Since the onion routers go about as mix routers, it is difficult to take after the method for a data packet through the framework.

The Anonymizer[13] proposed, Swarms conforms a re-routing structure for anonymous web browsing. This structure focuses on guaranteeing against particular enemies, for instance, the web server, or various bargained routers. It doesn't oblige encryption methods, because it relies on upon it to be set up in differing administrative ranges. In this way no grouped has an around the world framework see over all. The Anonymizer organization has a relative goal, whereby customers need to trust the single organization supplier.

M. Talasila, R. Curtmola, and C. Borcea[14] proposed Location verification through Immediate Neighbors Knowledge (LINK) thwarts attacks from individual malicious claimers or malicious verifiers. It also detects attacks involving groups of colluding users. Privacy and security analysis : the system also monitor users and requires their credentials to authenticate the proof. In other terms, users are not anonymous regarding the system.With pervasive computing, though, the scale of the problem changes entirely. Stefan Saroiu, Alec Wolman [15] presents location proofs a fundamental framework that enables the ascent of mobile applications that oblige "proof" of a customer's location. An location confirmation is a touch of information that guarantees a recipient to a geological location. Location proof is given out by the remote base to cell phone. The by and large short extent of the remote radios ensures that these gadgets are in physical region to the remote transmitter. In like manner, these devices are capable of exhibiting their present or past location to mobile application. The investigation identified with the security issue wherein a database ought to blessing access to figure genuine limits on the data records just under the condition that the outcomes don't reveal any specific data record.

In [16] proposed a customized k- anonymity model for giving location security. Our model grants mobile clients to describe and adjust their location protection particulars at the granularity of single messages, including the minimum anonymity level need, and the lapse resistances along the transient and spatial estimations. It has been developed a powerful message motor to execute this model. VeriPlace [17] is a location structural architecture structural planning with customer protection as a key setup segment.

III. . IMPLEMENTATION DETAILS

A. *System Overview:*

In this framework mobile users can gather location base tokens from the token merchants, and afterward trade their gathered tokens at token authorities for gainful prizes. Framework adds to a security and protection mindful location based compensating protocol for the LocaWard framework, and demonstrates the fulfilment and soundness of the protocol. Besides, framework likewise demonstrates that the proposed framework is fit to versatile different assaults and portable client security can be well ensured. Likewise for the security reason in our framework the trusted outsider who at first validate or enrolled the versatile clients follow the IMEI number of the portable client.

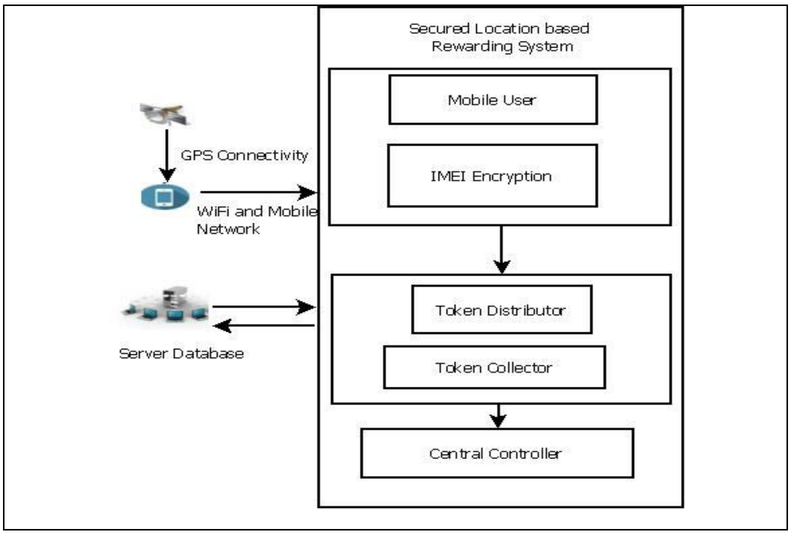

Fig. 1 shows the proposed system architecture.

At the point when the versatile client demand for the token to the token wholesalers, token merchant checks the IMEI number of the portable client, token authority likewise checks the IMEI number of the portable client when versatile client demand for token to the token gatherer. In the proposed framework recognize an assault by following the IP address of the attacker.

In token recovery, a token gatherer first checks whether the current MU endeavouring to redeem a token is a genuine structure client, without knowing its authentic ID. At that point, the token gatherer confirms whether the token to be recovered is set up and has not been changed since it was created with the organization of the CC, without important the conciliated of the token. After that, the token gatherer checks if the token does fit in with the MU. On the remote possibility that the MU passes all these confirmation stages, the token authority affirms whether the nature of the token ensured by the MU is exact, and gave that this is genuine, assigns the anticipated prize to him/ her. Along these lines, in our future system, no exceptional else other than the TTP can know a MU's certified character. As the CC and token authority simply have the information of token tryout information, they try not to have the foggiest thought regarding the substance of any token. Since a token authority/ wholesaler token is only aware of the location of the tokens it issued/recognized likewise there is no central server to store all the chronicled location information, no component could comprehend any specific MU's location history.

B. Algorithm:

System used RSA algorithm to encrypt the IMEI number of mobile user and one symmetric key, in RSA algorithm.

1) Each user generates a public/private key pair.
2) By selecting two large primes at random p and q.
3) Computing their system modulus N = p.q noteΦ (N)=(p-1)(q-1)
4) Selecting at random the encryption key e Where $1 < e < ø(N)$; gcd(e; ø(N)) = 1
5) Solve following equation to find decryption key de.d=1 mod Φ (N) and $0 \leq d \leq N$
6) Publish their public encryption key: KU = {e. N}
7) Keep secret private decryption key: KR = {d, p, q}

C. Mathematical model:

Let S, be a system such that
S = {fI, e, In, Ou, T, f_{me}, DD, NDD, ffriend, MEM_{shared}, $CPU_{CoreCnt}$, φ}

S- Proposed System
I- Initial state at T <init> i.e. Mobile user Login.
e-End state of reward used by mobile user.
X- Input of System i.e. Location ID
Y-Output of System i.e. Reward.
T- Set of serialized steps to be performed in pipelined machine cycle. In a given system serialized steps are Input, central controller, reward generate, token distributor, request for reward, etc.
f_{me}- Main algorithm resulting into outcome Y, mainly focus on success defined for the solution. In a given system RSA algorithm.
DD- Deterministic Data, it helps identifying the load-store function or assignment function. E.g. i= return i. Such function contributes in space complexity. In a given system deterministic data will be Reward generated by the central controller.
NDD- Non Deterministic Data of the system to be solved. These being computing function or CPU time or ALU time function contribute in time complexity. In a given system we need to find time required to generate tokens.
Ffriend- Set of satellite images.
MEM_{shared}- Memory required processing all these operations, memory will allocate to every running process.
$CPU_{CoreCnt}$- More the number of count doubles the speed and performance.
φ- Null value if any.

D. Experimental setup:

The framework is manufactured utilizing Java framework (version jdk 6) on Windows platform. The Net beans (version 6.9) are utilized as a development device. The framework doesn't require any particular hardware to run, any standard machine is fit for running the application.

IV. RESULT AND DISCUSSION

A. Dataset:
This system did not use any precise dataset. The requests for rewards are saved in the middle controller.

B. Results:

In this section we discussed the time required for processing when the user request for rewards and tokens. In the following table total time required is evaluated. In the table we have get token at client, get token at server, redeem token at client and redeem token at server. Table represents all type of time in milliseconds for each mobile user arrival rate.

Table 1: Time Processing Table

In Percent	Get Token at Client	Get Token at server	Redeem token at client	Redeem token at server
100%	197	101	286	101
200%	220	128	204	106
300%	232	137	254	171
400%	178	97	335	131

DOI: 10.15680/ijircce.2015.0306086

The following graph is plot from the values of above table. In X axis represent iteration number and Y axis represent average time in ms. The graph represent the values for four parameter get token at client, get token at server, redeem token at client and redeem token at server.

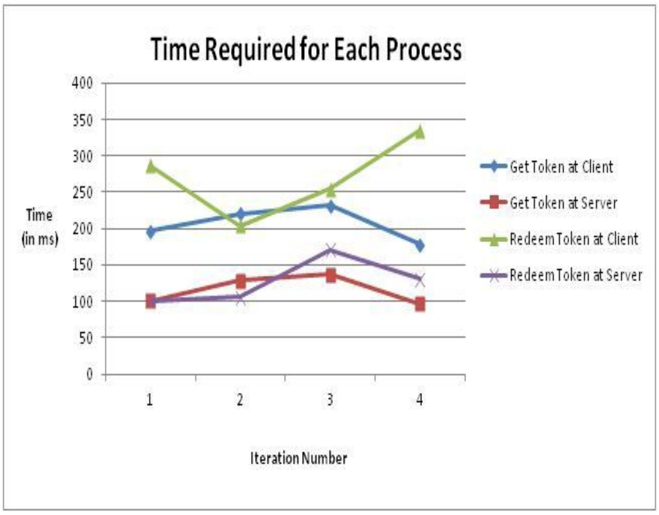

Fig.2: Processing Time Graph

IV. Conclusion and Future Work

A protected, protection safeguarding, and reasonable area based rewarding strategy is proposed. Framework have arranged a security and protection protocol for the structure The system is impenetrable to various sorts of attacks and compact client’s insurance can be acceptably guaranteed. The structure is adaptable to various sorts of attacks and versatile customers insurance can be all around secured also. It is invaluable for a few applications in which adaptable customers make substance to have the ability to affirm the commencement location and time of the substance. In future, rewarding methods can be summed up to address security and insurance issues by and extensive area based organizations and diverse zones like circulated processing.

References

1. Ming Li, “LocaWard: A Security and Privacy Aware Location-Based Rewarding System”, IEEE Transaction on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.
2. D.W. Gage, Lifelog,”Practical robotic self-awareness and self-knowledge”, Jan. 2004.
3. BugraGedik,”A Customizable k-Anonymity Model for Protecting Location Privacy”.
4. BugraGedik, ”Protecting Location Privacy with Personalized k- Anonymity: Architecture and Algorithms”, IEEE Transaction on mobile computing, Vol. 7, no. 1, January 2008.
5. YrjoRaivio, “Mobile Networks as a Two-Sided Platform - Case Open Telco” , Journal of Theoretical and Applied Electronic Commerce Research ISSN 07181876 Electronic Version Vol 6 / Issue 2 / August 2011/ 77-89 2011.
6. M. Gruteser and D. Grunewald, “Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking”, Proc. ACM Intl Conf. Mobile Systems, Applications, and Services (MobiSys 03), 2003.
7. Naveen Sastry, Secure Verification of Location Claims, ACM 1-58113- 769, San Diego, California, USA, September 19, 2003.
8. HuiZang and Jean Bolot, “Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study”, MobiCom’11, September 19–23, 2011, Las Vegas, Nevada, USA.
9. SastryDuri, Marco Gruteser, Xuan Liu,.”Framework for security and privacy in automotive telematics”,. In Proceedings of the second international workshop on Mobile commerce, pages 2532. ACM Press, 2002.
10. M.L. Yiu, C.S. Jensen, X. Huang and H. Lu, ”Space Twits: Managing the Trade-offs Among Location Privacy, Query Performance and Query Accuracy in Mobile Services”, Proc., 24th Int’l Conf. Data Eng., pp. 366-375,2008.
11. M. Gruteser and D. Grunwald, “Anonymous Usage of Location Based Services through Spatial and Temporal Cloaking,”Proc.First Int’l Conf. Mobile Systems, Applications and Services, pp. 31-42, 2003
12. Wanying Luo, “Proving Your Location Without Giving up Your Privacy”, ACM 978-1-4503-0005-6/10/02, February 2223, 2010.
13. Anonymizer. Anonymizer website.5694 Mission Center Road 426, San Diego, CA92108-4380, http://www.anonymizer.com, 2000.
14. M. Talasila, R. Curtmola, and C. Borcea.” Link: Location verification through immediate neighbors knowledge,” Mobile and Ubiquitous Systems: Computing, Networking,and Services, volume 73 Springer Berlin Heidelberg, 2012.

15. Stefan Saroiu, Alec Wolman, “Enabling New Mobile Applications with Location Proofs”, ACM 978-1-60558-283-2/09/02, February 23-24, 2009.
16. B. Gedik and L. Liu, “Protecting Location Privacy with Personalized K-Anonymity: Architecture and Algorithms”, IEEE Trans. Mobile Computing, vol. 7, no. 1, pp. 1-18, Jan. 2008.
17. Wanying Luo, “VeriPlace: A Privacy-Aware Location Proof Architecture”, ACM GIS 10, November 25, 2010

BIOGRAPHY

Prerna Wankhede(Patil) is P. G. Scholar in the Computer Engineering Department, TSSM’s BSCOER,Narhe,Pune. She has received Bachelor of Engineering (B.E.) in Information Technology from RTMNU (Nagpur University) ,India. She is currently working as Lecturer in MIT Polytechnic, Kothrud, Pune. Her research interests are Security and software engineering.

Prof. M. K. Kodmelwar is a full time Assistant Professor at Department of Computer, TSSM’s BSCOER,Narhe,Pune, India.He has 14 years of experience in teaching. He has perusing Ph.D in Computer Science and completed his Master degree from Bharati Vidyapeeth.Pune and his research interest is computer network.

DOI: 10.15680/ijircce.2015.0306086