# GEO HASH BASED LOCATION PROTECTION

**Anjali Anand[1], Shobha T[2]**

*[1]M.Tech, Department of Computer Science & Engineering, The Oxford College of Engineering,*
*[2]Associate Professor, Department of CSE, The Oxford College of Engineering*

## Abstract

*Cell phones and the Internet have changed the correspondence and with it the lifestyle of people. This project aims to shield area security in Geo-Social Applications alongside a component of following along surveyed information. The point of this paper is to grasp territory based organizations (LBS) and recognize its key parts behind organization giving then shed some light on the limitation keeping the development movement. This project aims at providing a system for safeguarding location privacy in Geo-Social Applications along with a feature of tagging along polled data.*

***Keywords:*** *GEO- Social Application, Location Protection, Territory Based Organizations, Safeguarding Location.*

---------------------------------------------------------------------***---------------------------------------------------------------------

## I. INTRODUCTION

A growing number of cell phones and Personal Digital Assistants (PDA) license people to get to the Internet wherever they are and at whatever point they require. The presence of various innovations, for example, remote systems, Internet, Geographical data frameworks (GIS) and Global Positioning Systems (GPS), have presented another sort of data innovation called Location Based Service (LBS). The presence of various advances, for example, remote systems, Internet, Geographical data frameworks (GIS) and Global Positioning Systems (GPS), have presented another kind of data innovation called Location Based Service (LBS).Location Based Services or geo-social applications is characterized as the capacity to find a versatile client topographically and convey administrations to the client taking into account his area.

With the growing usage of geo-social applications, a convenient way of sharing location with friends, the need to have a system that preserves the privacy of the location of the user also arises. Friends on the geo-social application share their location with each other, however this can hamper their privacy, which can lead to very harmful consequences such as stalking, home invasion and other crimes. There is a probability of security infringement by noxious clients. In the proposed project, users registered on the application , share their location with their friends along with a secret key which is generated by an AES algorithm.

The project focuses on an approach that does not compromise on the security while fully taking advantage of the geo-social applications. In this approach, Friends share their location with one another, the location is identified in terms of latitude and longitude co-ordinates, these co-ordinates are scrambled, before putting away them on untrusted servers. The security is further upgraded by presenting a caution framework, where by an interloper can be followed. This project also introduces an approach that display necessary and useful information to a user while accessing his friends location via secret key. The useful information is based on the friends location coordinates. This is done by a method of tagging polled data.

## II. RELATED WORK

Geo- social applications offer a convenient approach for people to know more about their surroundings. There are many popular geo social applications, however these location based services(LBAS) reveal the exact location of the user, and this could be a threat to the privacy of the location of the user, which could have many harmful consequences such etc as home invasion, stalking and hence we need to enhance the privacy as for the area of the client.

Stefan Steiniger, Moritz Neun and Alistair Edwardes [1], Location Based Services (LBS) are turning out to be quickly in the versatile and data improvements (IT) fields.Build interest to cutting edge innovations and enthusiasm for using geospatial data servers to give helpful data and administrations to portable clients however remote systems plays an essential component to LBS progression.

Thamer Abulleif & Abdulwahab Al-Dossary [2], GPS is the overall satellite-based radio route framework, comprising of 24 satellites, just as separated in six orbital planes 20,200 kilometers over the Earth, that transmit two uncommonly coded bearer signals, one for non military personnel use and one for military and government use.

LBS offers extraordinary opportunities to know the surroundings but at the same time raises challenges on privacy enhanced technologies [3]. This is need for privacy is well illustrated in the article “Location Privacy in Web Based LBS” By Maria Luisa Damiani. In this position paper the discourse with a few contemplations have been added. The author of this paper has elaborately described the motivation to enhance the users awareness in terms of location privacy.

Manav Singhal, Anupam Shukla[4], Region based Services offer various purposes important to the convenient customers to recoup the information about their present range and method that data to get more supportive information near their zone.

Existing frameworks have principally taken many ways to deal with enhancing client protection in geo-social frameworks [5], by presenting instability or blunder into area information. In this paper, Ling Liu proposed “A Personalized Anonymization Model”, This paper portrays a customized k-obscurity model for securing area protection against different protection dangers through area data sharing. Be that as it may, this has two drawbacks. To begin with, low spatial determination in area irritation might lead the LBS supplier to give more coarse grained area subordinate data to the portable client, which might weaken the quality of the service. Second, the additional postponement presented through transient shrouding of area data might diminish the apparent administration quality of the portable client.

Hence an alternative approach that aimed at increasing Location Privacy via Private Proximity Testing[6]. This approach empowers a couple of companions to be informed when they are inside of a limit separation of each other, however something else uncover no data about their areas to anybody. This method allows two friends on the same application know how close they are to each other without revealing their location.

## III. SYSTEM DESIGN

The disadvantages of the above works have left a scope of improvement in location privacy in geo social application which is the prime focus of this project by means of a prototype application. This project focuses on area security, a specific kind of data security that we characterize as the capacity to keep different gatherings from learning one's present or past area.In the proposed project, users registered on the application , share their location with their friends along with a secret key which is generated by an AES Algorithm. A user shares his location with his friends, and when the friend wants to access the location , he enters the secret key and views the location. The secret key is share via email.Area data is commonly controlled by an area data source, for example, GPS collector in a vehicle. Once the GPS receives the latitude and longitude information, the latitude and longitude values are scrambled before putting them away on trusted servers[7]. These Trasnformations are made by implementing the Advanced Encryption Standard Algorithm [AES][8][9][10]

AES depends on an outline rule known as a substitution-change system, blend of both substitution and stage, and is quick in both programming and hardware. Unlike its forerunner DES, AES does not utilize a Feistel system. AES is a variation of Rijndael which has an altered square size of 128 bits, and a key size of 128, 192, or 256 bits. By difference, the Rijndael particular in essence is determined with piece and key sizes that might be any different of 32 bits, both with at least 128 and a greatest of 256 bits .Once the encrypted values of a location is stored on the trusted servers, they can be decrypted only by a secret key.

This project enforces a third level of security that incorporates a system where the users on the Mobile geo-social applications could receive an alert if an intruder is trying to access their location, and the intruder can be traced. For instance, information scrubbers might work surreptitiously through concealed projects, or they might join with a fake email address keeping in mind the end goal to get individual data from clueless clients[11].

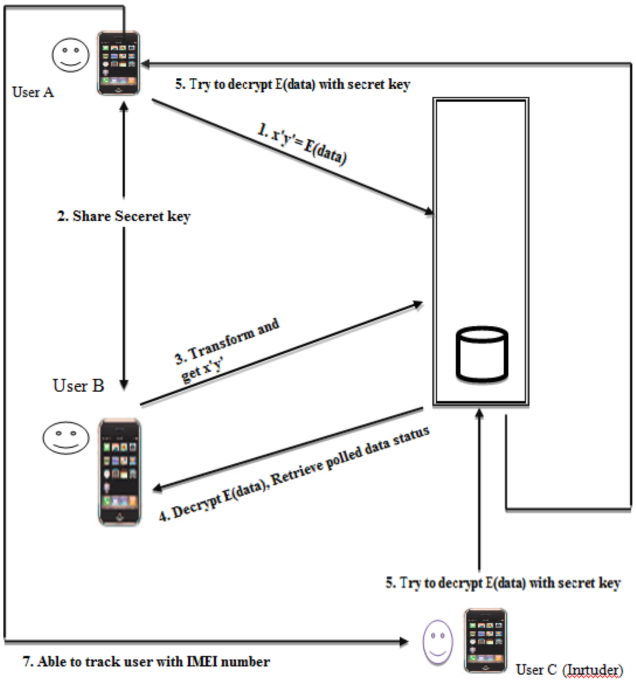

User A
5. Try to decrypt E(data) with secret key
1. x'y'=E(data)
2. Share Seceret key
3. Transform and get x'y'
User B
4. Decrypt E(data), Retrieve polled data status
5. Try to decrypt E(data) with secret key
7. Able to track user with IMEI number
User C (Inrtuder)

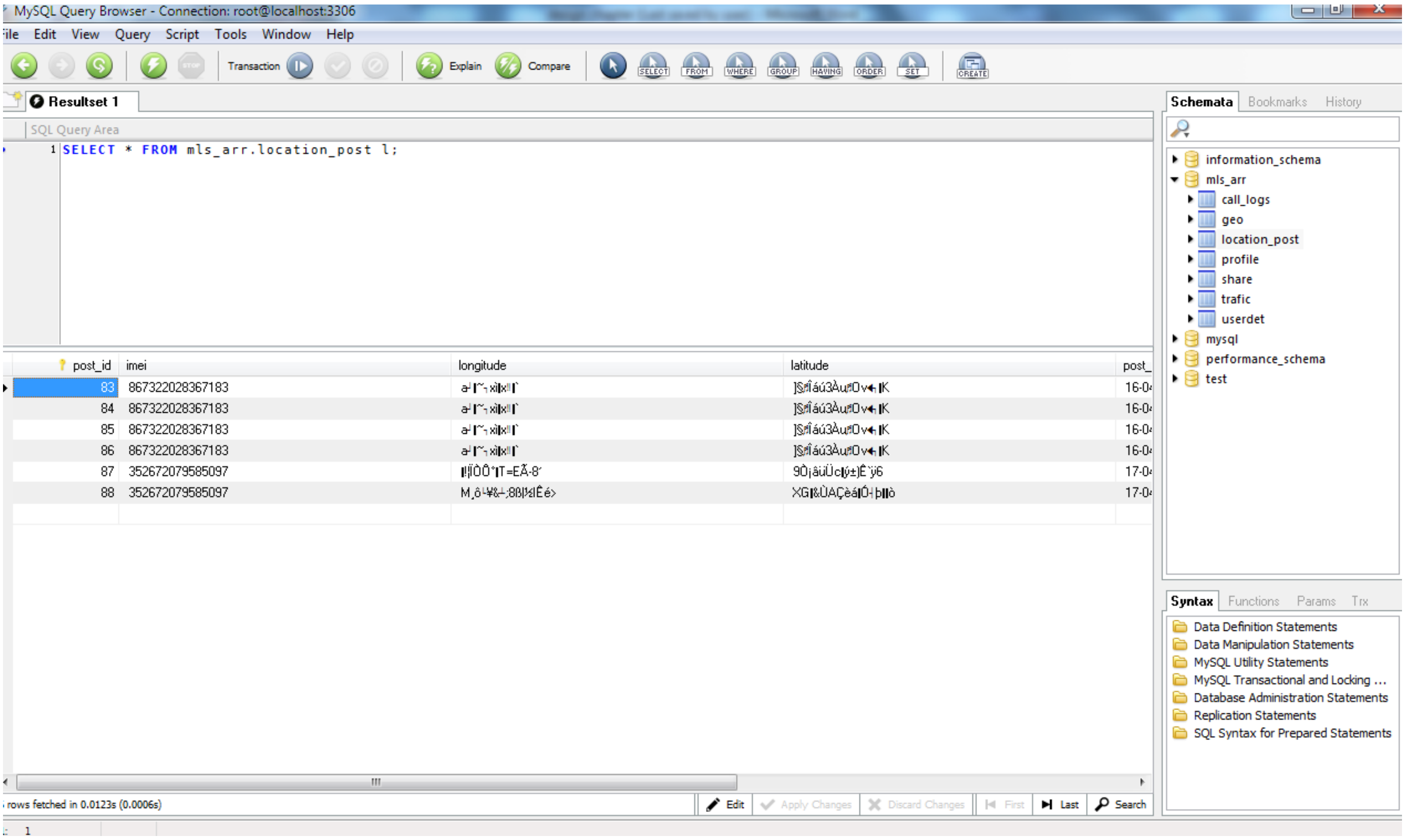
**Fig 1:** Architecture of Geo Hash based Location protection

This project also introduces an approach that display necessary and useful information to a user while accessing his friends location via secret key. The useful information is based on the friends location coordinates. This is done by a method of tagging polled data. The proposed framework fuses the idea of information examination where by clients can misuse the utilization of surveyed information to know the present situation at the specific area they are getting to [12].

## IV. EXPERITMENT RESULTS

The Experimental results stage is to decipher the outline of the framework delivered amid the configuration stage into code in given programming dialect. User's current location information obtained from the positioning component (in this example, GPS data), is sent to service server via the mobile communication network. The latitude and longitude values are scrambeled before putting them away on the server. These changes are performed utilizing cryptographic hash capacities. The area directions are scrambled by the 128 piece AES encryption plan and the encoded qualities are put away on trusted servers. A mystery key is then created and sent to the companions email.

The receiver of the secret key then decrypts the location details. When the user shares the location with his/her partner, he/ she also selects the status of his location for example if there is an ongoing strike or an emergency probably an accident or the location status could also describe a traffic jam. After selecting the particular area status and sharing it with the area details, then the partner decrypts the area details and also gets to know the status of the particular area.


MySQL Query Browser - Connection: root@localhost:3306
File Edit View Query Script Tools Window Help
Transaction
Explain
Compare
SELECT FROM WHERE GROUP HAVING ORDER SET CREATE
Resultset 1
SQL Query Area
Schemata Bookmarks History
information_schema
mls_arr
call_logs
geo
location_post
profile
share
trafic
userdet
mysql
performance_schema
test
Syntax Functions Params Trx
Data Definition Statements
Data Manipulation Statements
MySQL Utility Statements
MySQL Transactional and Locking ...
Database Administration Statements
Replication Statements
SQL Syntax for Prepared Statements
Edit Apply Changes Discard Changes First Last Search

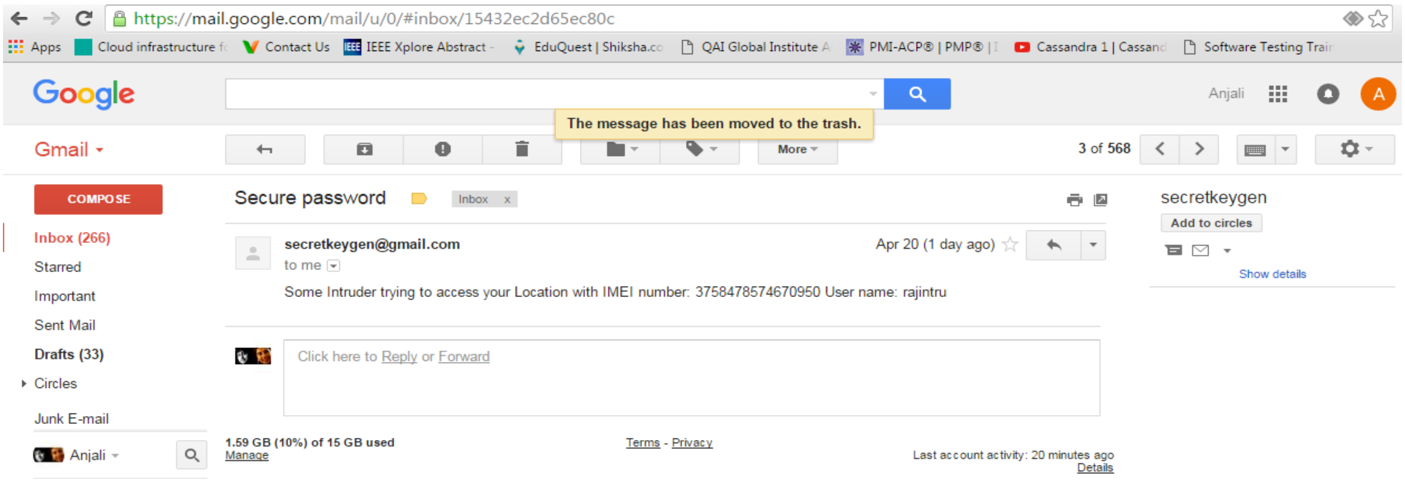
```
1 SELECT * FROM mls_arr.location_post l;
```

| post_id | imei | longitude | latitude | post_ |
|---|---|---|---|---|
| 83 | 867322028367183 | a┘▌˜┐xì▌x‼▌` | ]§╡Îáú3Àu╡0v◂▌K | 16-0 |
| 84 | 867322028367183 | a┘▌˜┐xì▌x‼▌` | ]§╡Îáú3Àu╡0v◂▌K | 16-0 |
| 85 | 867322028367183 | a┘▌˜┐xì▌x‼▌` | ]§╡Îáú3Àu╡0v◂▌K | 16-0 |
| 86 | 867322028367183 | a┘▌˜┐xì▌x‼▌` | ]§╡Îáú3Àu╡0v◂▌K | 16-0 |
| 87 | 352672079585097 | ▌‼ÎÒÔ˚▌T=EÃ-8´ | 9Ò¡âüÜc▌ý±)Ê`ÿ6 | 17-0 |
| 88 | 352672079585097 | M¸ô┘¥&┴;8ß▌½▌Êé> | XG▌&ÙAÇèá▌Ó┤þ▌▌ò | 17-0 |

rows fetched in 0.0123s (0.0006s)

**Fig 2:** Transformation on Location coordinates

A third level of security is enforced when an intruder logs into the database and gets hold of the secret key, however when he tries to log in with that secret key, he is restricted to view the location and an alert with the imei number of the intruder is sent to the user who shared his location.


https://mail.google.com/mail/u/0/#inbox/15432ec2d65ec80c
Apps Cloud infrastructure f Contact Us IEEE Xplore Abstract - EduQuest | Shiksha.co QAI Global Institute A PMI-ACP® | PMP® | I Cassandra 1 | Cassand Software Testing Trair
Google
Anjali
A
Gmail
More
3 of 568
COMPOSE
Inbox (266)
Starred
Important
Sent Mail
Drafts (33)
Circles
Junk E-mail
Anjali
Inbox x
secretkeygen
Add to circles
Show details
1.59 GB (10%) of 15 GB used
Manage
Terms - Privacy
Last account activity: 20 minutes ago
Details

The message has been moved to the trash.

Secure password

secretkeygen@gmail.com Apr 20 (1 day ago)

to me

Some Intruder trying to access your Location with IMEI number: 3758478574670950 User name: rajintru

Click here to Reply or Forward

**Fig 3:** Tracking an intruder

## V. CONCLUSION

This project report provides an analysis and evaluation of the current Location based system and proposes a new system that is more secure. Initially mobile phones were developed only for voice communication but now a days the scenario has changed, voice communication is just one aspect of a mobile phone. There are other aspects whichare major focus of interest. Two such major factors are web browser and GPS services.This Project Implements these factors in a very secure way, Hence this project aims at providing an approach that preserves the location of the user while fully taking the advantage of the geo-social applications. Friends Share their location with one another, the location is identified in terms of latitude and longitude co-ordinates, these co-ordinates are encrypted, before storing them on untrusted servers.

When a friend shares the location with another friend they share a secret key via email, and when the friend tries to access the location , only if he keys in the correct secret key he will have access to view the location of the friend. This project enforces a third level of security that incorporates a system where the users on the Mobile geo-social applications could receive an alert if an intruder is trying to access their location, and the intruder can be traced.

This project also introduces an approach that display necessary and useful information to a user while accessing his friends location via secret key. The useful information is based on the friends location coordinates. This is done by a method of tagging polled data.

## REFERENCES

[1] Stefan Steiniger , Moritz Neun , Alistair Edwardes, “Foundations of Location Based Services”.

[2] Thamer Abulleif & Abdulwahab Al-Dossary ,” Implementing Location Based Services” InInternational Journal of Computer Science Issues, January 2010

[3] Maria Luisa Damiani 1 and Pierluigi Perri2 ,”Location privacy in web-based LBS”, position paper 2011.

[4] Manav Singhal and Anupam Shukla,”Implementation of Location based Services in Android using GPS and Web Services”, International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012

[5] Ling Liu, Bu˘gra Gedik,” Location Privacy in Mobile Systems: A Personalized Anonymization Model”.

[6] Arvind Narayanan Narendran Thiagarajan Mugdha Lakhani, Michael Hamburg Dan Boneh” Location Privacy via Private Proximity Testing”.

[7] Krishna P. N. Puttaswamy∗, Shiyuan Wang, Troy Steinbauer,Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel and Ben Y. ZhaoPreserving Location Privacy in Geo-Socia Applicationsl IEEE Transactions On Mobile Computing Vol:13 No:1 Year 2014

[8] Hatem Hamad and Souhir Elkourd, “ Data encryption using the dynamic location and speed of mobile node”. Academic Jouranls, 2010.

[9] Avi Kak AES: The Advanced Encryption Standard Lecture Notes on “Computer and Network Security” Lecture notes April 2016.

[10] William Stallings, “Cryptography and Network Security”, Fourth Edition.

[11] A.Lutarsky ,”Protect your information from intrusion detection”

[12] Chen-Khong Tham and Tie Luo,”Quality of Contributed Service andMarket Equilibrium for Participatory Sensing”IEEE Transactions On Mobile Computing, Vol. 14, No. 4, April 2015