Locus Guard Pilot

Locus Guard Pilot

Varsha Chandrashekar, and Prabadevi B

Vellore Institute of Technology, Vellore-632014, Tamilnadu, India

Email: prabadevi.b@vit.ac.in

Abstract. Providing services to user is the main functionality of every search engine. Recently services based on users' current location has also been enabled with the help of GPS in every smartphone. But how safe are their searches and how trustworthy is the search engine. Why are users tracked even when they turn off the tracking. Where lies the solution. Unless there is a security system to prevent ad trackers from misusing user's location, any application which relies on user's location will be of no use.

We know that location information is highly sensitive personal data. Knowing where a person was at a particular time, one can infer his/her personal activities, political views, health status, and launch unsolicited advertising, physical attacks or harassment. Therefore, mechanisms to preserve users' privacy and anonymity are mandatory in any application that involves users' location.

So there comes the need to hide the location of the users. This proposed application aims to implement some of the features required for preserving users' privacy and also a secure user login so that services provided to users can be used by them without danger of their searches being misused.

1. Introduction

As location-enabled mobile devices proliferate, location based services are rapidly becoming immensely popular. Most of the current location-based services for mobile devices are based on users' current location. Users discover their locations and share them with a server. In turn, the server performs computation based on the location information and returns data/services to the users. One good example of such location based services are search engines which not only track the searches of users and provide services based on user's current location but also allow ad trackers to fulfill their needs. Finally, the user is affected due to these unnecessary ads and calls. So there comes the need to find a solution to this problem for preserving user's location privacy and at the same time fulfilling their needs.

1.1. Ease of Use

Selecting the type of search for users is provided. Unlike other search engines, in LGP users can search the object by selecting their type of search. Finding the user searches count through this platform. While the users privacy is preserved , yet the database entities can find the number of times a particular user has made a search using LGP.

2. Related work

Wandex is found to be the first Web robot and search engine established in 1993. AltaVista and Excite were some of the previous search engines but they followed the traditional information retrieval techniques [1].

Google Maps and Yahoo Local are two next big engines, which quickly changed the search engine usage, and attracted masses.Then emerged the world examples of commercial location-aware search engines. However, these engines used Yellow Pages to search the queries and their location-based services were limited to few countries, though now they have updated [2].

Asadi et al. in 2006 proposed Target location, which considers the location of the users or web resource users. However, the access to such data and estimation of the scope is difficult for search engines [3].

Duck duck go is the private search engine that came in 2008 that enabled users to search for anything with utmost security and privacy that Duck duck go itself doesn't know who you are and has no history of your searched unlike Google which encrypts search traffic when logged in, but this only prevents third-parties from snooping on your search traffic – it doesn't prevent Google from tracking you [4].

But there is also a need for secure login for providing location based service safely only to registered users and what better example than the concept STAMP proposed by Xinlei Wang,Amit Pande, Jindan Zhu, and Prasant Mohapatra [5].

3. System Model and Framework

We propose a novice system that acts as a privacy preserving search engine that uses location based services to provide users with best information from resources.The searches made by the users are also categorized into normal, virtual and lbs based. This paper proposes a technique to retrieve their query from database and further enhance the results.

Initially once the user registers in the application,the verifier will verifies the users account by checking if the current location matches users registered location.Then the certificate authority checks all details and verifies the account.Only after this can the user log in to the application to perform the searches. The geolocation API helps users to track their current location and provide services from the neighbourhood based on the type of search performed under lbs search that is we divide the entities into categories.The lbs search is divided into poi search and virtual search. Under poi, there are options to Select category such as malls, temples, restaurant, park, theatres. Similarly under virtual there are options to search for a service example laptop and then choose the category for the laptop such as hp to find the nearby service stations for hp repair or maintenance.

So now how is the privacy protected for these searches.Hence we have to encrypt the searches performed by the user such that neither any hacker who hacks into the application will be able to view it nor the admin in our case the verifier and ca. So the searches are secure and privacy is protected.But there are already search engines such as duck duck go which perform a similar functionality. So how are we different.Well, we are aware that to appear as the first in the searched query executed by the user, the entity needs to pay the search engine. Also a particular search though protected by some engines, the website that links to that search may not necessarily work in a similar way. It could track your location and the searches performed internally. Here the engine cant pave way to its claim of completely protecting users privacy. So the result for the query comes from the database. A database that is updated every day by the user to display the offers and speciality for that day. Again now how will that website in our case the entity of that table as a person know that its users actually use this engine for its searches? Therefore, we give the owner the access to view the searches and the count and further related information of the users as required by the entity. This we provide by decrypting the encrypted data in the database.

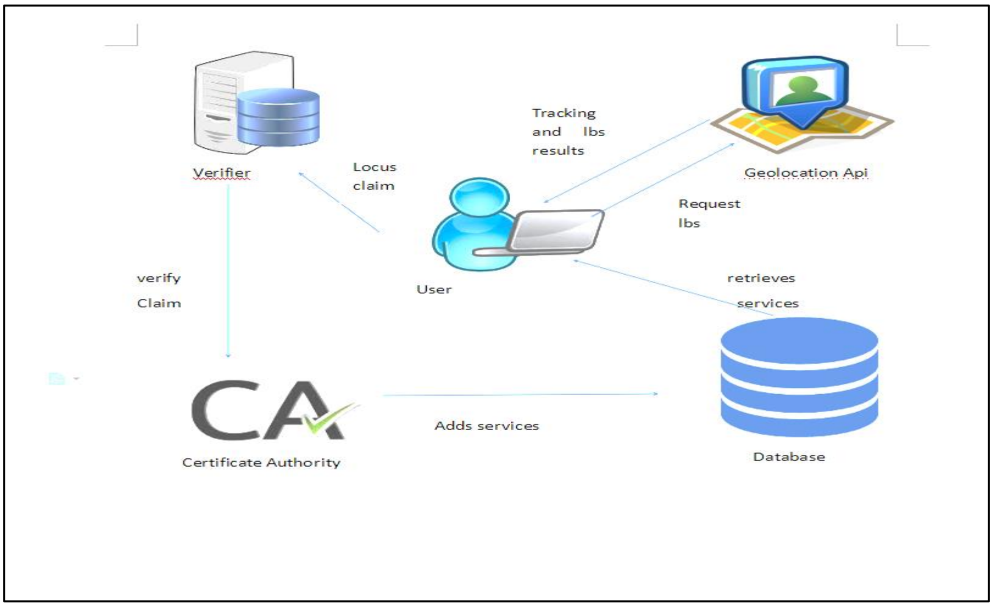


Fig. 1. System Overview

4. System Overview

The system contains the three major entities user, certificate authority and verifier whose roles will ensure that the system functions securely as desired. These entities are depicted in the figure Fig.1

Initially, there are three entities of this app. The verifier, certificate authority and the user.

Step 1: The user first signs up to use this secure searching app.

Step 2: The current location of the user is tracked to complete the sign up process.

Step 3: The verifier logs in

Step 4: The verifier will verify details

1) Checking current latitude and longitude with the users signed up location

2) Verify the user for certificate authority

Step 5: The certificate authority will now verify the details and activate the user.

Step 6: Only after the verifier and ca activate the user, the user can now login to the app.

Step 7: Now the user can perform different types of search:

POI search-This is for location search where the latitude and longitude of current location is captured and compared with stored latitude and longitude and at the point of intersection, the geo location api retrieves the nearby places.

Virtual search- This is for the category of items.

Normal search- This is for any item in the database.

The safety of this search is ensured by encrypting the locations searched.This encryption can be done through:

1. Bit exchange method
2. AES encryption

4.1. Bit exchange method

Input: query (location)
Output: crypt text
Variables: String crypto, cleartext
Assumptions: User types in a valid query

Encryptions taken on the secret message file using simple bit shifting and XOR operation. The bit exchange method is introduced for encrypting any file.

Steps:

1. Read one by one byte from the secret data and convert each byte to 8 bits. Then apply one bit right shift operation.
2. Divide the 8 bits into to blocks and then perform XOR operation with 4 bits on the left and 4 bits on the right side.
3. The same thing repeated for all bytes in the file.

Example: If query is vellore

Then for each letter find its ascii

So V will be 118 which is 0111 0110 in binary

0	1	1	1	0	1	1	0

Perform 1 s complement to the above binary code.

1	0	0	0	1	0	0	1

Now divide this code.

1	0	0	0
1	0	0	1

Now XOR the above 2 codes

$$\begin{array}{c} 1000 \\ \oplus \\ \underline{1001} \\ 1010 \end{array}$$

The xor result is: 1010

Now the combination of xor result with the right side bit will give final result

Now final result is : 10101001

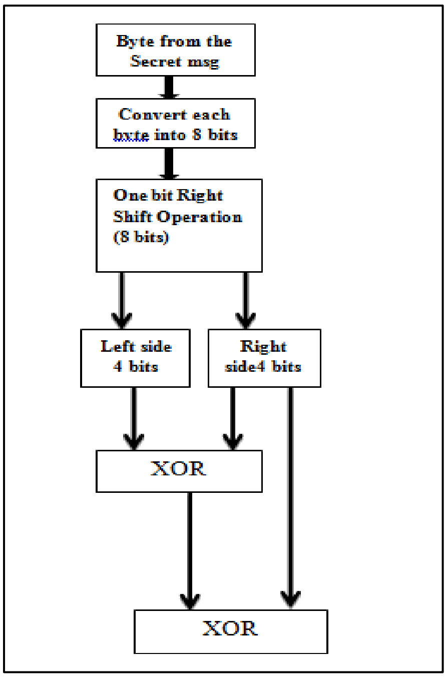

Byte from the Secret msg
Convert each byte into 8 bits
One bit Right Shift Operation (8 bits)
Left side 4 bits
Right side4 bits
XOR
XOR

Fig. 2. Bit Exchange Method

4.2. AES algorithm

Input: query(location)

Output: crypt text

Variables: String str, str1

Assumptions: User types in a valid query

AES (acronym of Advanced **Encryption** Standard) is a symmetric **encryption** algorithm. A method for encrypting and decrypting information. Thus it uses the same key for both encryption and decryption.A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10.

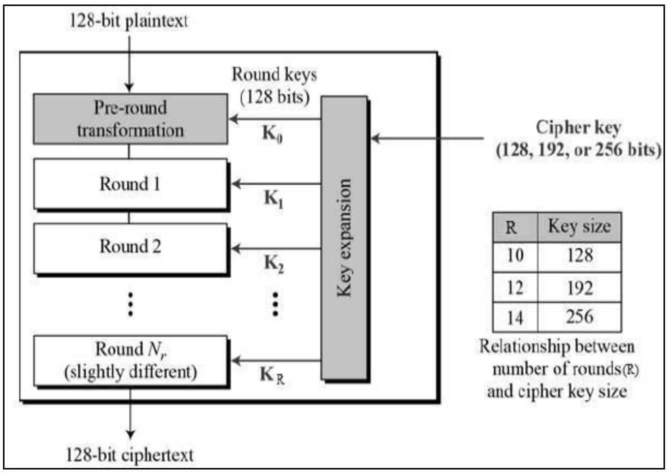


Fig. 3. AES Method

Steps:
The location of the user eg: vellore is the key in english.

Which is translated into hex, So vellore will become 118 101 108 108 111 114 101

Now this decimal is converted to hex key.

118 - 76
101 - 65
108 - 6C
108 - 6C
111 - 6F
114 - 68
101 - 65

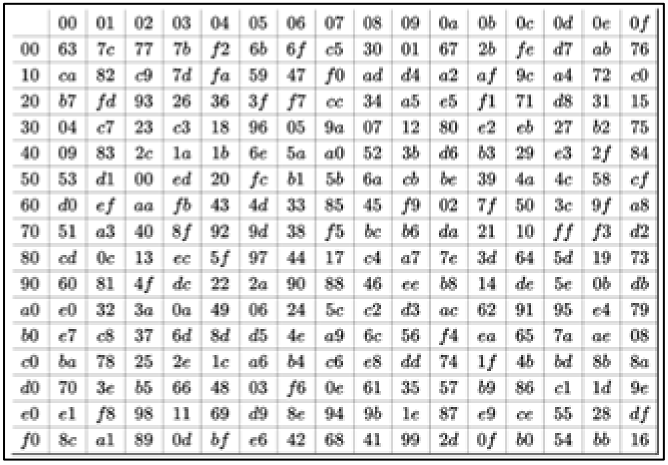
Key in Hex (128 bits):76 65 6C 6C 6F 68 65

w[0] = (76, 65, 6C, 6C)   w[1] = (6F, 68, 65, 00)

g(w[1]): circular byte left shift of w[1]: (68, 65, 00, 6F)

Byte Substitution (S-Box): (45, 4d, 63, 42)

Calculated from existing table depicted in Fig 4



	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig. 4. S-Box

Adding round constant (01, 00, 00, 00)
0100 0101
$\oplus$
0000 0001

0100 0100

gives:

g(w[1]) = (44, 4d , 63, 42)

w[2] = w[0] $\oplus$ g(w[1]) = (76, 65, 6C, 6C) $\oplus$ (44, 4d , 63, 42) = 32 28 F 2E

w[3] = w[2] ⊕ w[1] = (32 ,28, F, 2E) ⊕ (91, 12, 91, 88) = A3 3A 9E A6
w[4] = w[3] ⊕ w[2] = (A3 3A, 9E,A6) ⊕ (B1, 59, E4, E6) = 12 63 7A 40
w[5] = w[4] ⊕ w[3] = (12, 63, 7A, 40) ⊕ (D6, 79, A2, 93) = C6 1A D8 D3

first roundkey: 32 28 F 2E A3 3A 9E A6 12 63 7A 40 C6 1A D8 D3

Then we get the list of all roundkeys

Add Roundkey, Round 0
Round 1, Substitution Bytes
Round 1, Mix Column
Similarly we follow steps for all the rounds and get the cipher text.

The verifier logs in and checks history, he can see the name , query(location) in encrypted format, category, time stamp.

So neither the admin nor any hacker can find out the searched queries due to encryption used.

5. Implementation

The proposed system is implemented using java language with java server pages and html with javascript as front end and servlet as backend.We also store all the data which are regularly updated in mysql. We have used glassfish server.The working can be expressed with the modules described.

Login of CA : The certificate authority logs in to the application to provide services and activate user accounts.The user name and password are fixed for the ca as he being the admin can choose the name and password he desires.

Addition of services: The services are added into the database by the CA. The CA must also regularly update the Entries in the database as there may be new features or offers or change in address for a service.

Verification by verifier: The verifier logs in to verify the list of users by checking if their registered location matched their current location.

Activation: The activation takes place finally only by the CA after the verifier has verified the user. The CA will view all the registration details before activating.

User Login: Once activated , the user can login using the registered user name and password to perform location based searches and find the desired results.

Search: We have three types of search, the normal search which works like the searches performed by any other search engine, then the poi search which results in response with the places near the users current geographical position and ultimately the virtual search which displays services available nearest to the user. The user can choose the category and the list that is available nearest to the user is displayed. It also displays the distance from the current location to the one queried.

History of searched items: The history of the searches made is available for the verifier and ca to view. However, the query and the location of the user are hidden. The hiding happens through encryption. We have used bit-by-bit encryption as well as AES and made a comparative analysis as to see which one suits better.

Login of service owner: A separate web based app is developed to enable the service owner to view the decrypted data.

Display of the user searches: The encrypted query of the user and their latitude and longitude is decrypted and available to the owner for their analysis purpose.

6. Result and Analysis

The users can perform secure searches and the service owners can view how many times the user has used the lgp for searching their shop. The security of the users location and their searches is performed by the below two methods and we analyse the time taken to perform. Bit by Bit Encryption-runs by 38 seconds.AES Encryption-runs by 55 seconds.

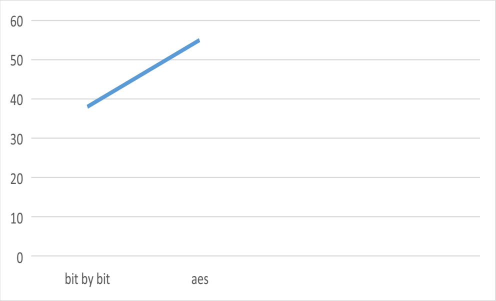


Fig. 5. Line graph

Line graph depicted in fig.5 is of time taken in seconds to perform the algorithms for the application.

Though there is a difference of 7 seconds , AES is more secure when compared to number of rounds for encrypting the data.

7. Conclusion

In this paper, we propose a way to search for any data securely without the nuisance of ads and tracking. The application allows users to not only search for a place or service near their geographical position using point of interest but also as a general search like any other normal search engine. As we know that location information is very valuable and needs to be taken into utmost caution in protecting it, so does the data the user searches for and this application claims to do both. Not just this, the service owners alone get to know the count of users or their identity in some genuine cases, but nobody else not even the app admin nor any hacker as all data is encrypted.

In future we will further develop our idea in the following aspects:

The service owners to customize offers to a frequently visited customer could use the history of searched items.

The matching of live image with the image available in the database from any of the identity proofs during registration with user name as the id in the proof and password as chosen during the registration process along with the current location being tracked as proposed already in this paper.

The user could communicate with the service owner for any doubts or requests for any offers on their service.

Acknowledgment

The authors faithfully pay their gratitude to the anonymous referees for their suggestions that have led to the presentation of this novel concept in this paper. We are also thankful to our university for the

invaluable resources that are in our access to increase our knowledge and help us participate in the learning process.

References

[1] http://encyc.org/wiki/Wandex

[2] Pasi Fränti, AndreiTabarcea and Juha Kuittinen 2010 *Location-based search engine for multimedia phones*, 2010 IEEE International Conference on Multimedia and Expo, Suntec City, Singapore.

[3] Asadi S,Xu J,Shi Y,Diederich J and Zhou X 2006 *Calculation of target locations for web resources.* Web Information Systems - WISE 2006. Lecture notes in Computer Science, vol **4255**. Springer,Berlin,Heidelberrg.

[4] https://en.wikipedia.org/wiki/DuckDuckGo

[5] Xinlei Wang, Amit Pande and Jindan Zhu, 2016 *STAMP: Enabling Privacy-Preserving Location Proofs for Mobile Users* IEEE/ACM Transactions on Networking , Vol: **24**, Issue: 6, Dec. 2016.