# Authenticate User Location using Auditor and Locate Nearest People

**Suryawanshi Sagar[1] Shaikh Shahebaz[2] Pagare Shekhar[3]**
[1,2,3]R. H. Sapat College of Engineering, Management Studies and Research, Nashik

*Abstract*— Services or applications based on location i.e. based on latitude and longitude are famous now days. Various business openings, start ups looking forward for this location based applications and incorporate them into their business models. The major criteria are, end user's location should be accurate and authentic. While validating the location of end user, his privacy must be preserved. Hence there must be designed protocol that uses the end user's location efficiently by preserving privacy. Hence system is designed in which authentic witness validates the end user's location and then respective services are provided to the user. Here idea of proposed system is that super user (administrator) manages the data regarding locations and witness who authenticate the location. When end user is on particular location and wants to share data, then he has to populate his location details. These location details are shared with the witness and after witness approval user can share date about that location. Other users can get data when they will be on that location. Proxy location can also be generated by end user to get data about different location. This system works on location based security aspect.

***Key words:*** Witness, latitude, longitude, location based system, proxy

## I. INTRODUCTION

LBS are well known services in daily routine. Various businesses are come with such LBS. These location based services should be appropriate from location accuracy point of view. User's privacy may be affected during validation of location of specific user. Therefore, we have to work on framework that correctly identifies location of user and also protect the privacy of particular user. We design our system in such way that it can be easily accessed by the user. Our system has some features like, maintainability, modularity and effectiveness. Location based services are popular in daily routine. Due this, LBS incorporate many businesses in it. These location based services should be appropriate as far as accuracy of location is concern. There are many cases in which user have to prove his location to another user or super authority. There is need of such system that validates the location that is share with the colleagues or various authorities. Our proposed system works on generating secure location attribution on the mobile devices. Our system validates Keywords- witness, location provenance, location based services, privacy protection against un-trusted user or third party. Our main contribution in this system is to preserve privacy of user while revealing his location to the server. It is achieved with the help of crypto-Id provided to the user and used in the protocol to represent the end user. Then manipulate location of user by avoiding barriers in communication. Also we have to make this framework more portable as far as devices are concern. In proposed approach historical order of proofs are also preserve. Therefore, attacker should not be able to change the order of proofs in the original records. The privacy of information within a proof is display with respect to the required user and an attacker or auditor should not be able to view any private information not intended to be exposed by the user. Proposed approach helps user to share data with the server about particular location. While uploading data about particular destination, user's location is verified by the authentic witness and user privacy is preserved and data is uploaded on successful verification. User can also generate proxy location if he wants particular information.

## II. RELATED WORK

"S. Saroiu and A. Wolman,"Enabling new mobile applications with location proofs," introduced location proof with android smartphones. They suggest a method which traced geographical locations of devices to generate location proofs. It can be manipulated when requirement checking is done for specific existed user.

"I.Maduako,"Wanna Hack a Drone? Possible with Geo-Location Spoofing!."" introduced spoofing of geo-location. Spoofing of Geo-location is an attempt to achieve GPS co-ordinates by propagating more powerful signal than received from the GPS satellites. It resemble structured to the group of original GPS signals. To show position other than original position spoofed signals are used. It is specifically seen by attacker. It is a serious issue for Unmanned Aerial Vehicles (UAVs). Spoofing of geo-location is major issue found in location based services as get those militaries drones

N. O. Tippenhauer, K. B. Rasmussen, C. Popper, and S. Capkun, "iPhone and iPod location spoofing: Attacks on public WLAN-based location provenance systems," represents location of iPhone user. It is manipulated by using its IP address of WLAN. Authors were studied about the security of public WLAN. It is based on positioning systems. Particularly, author was investigating Skyhook positioning system. This is available on PCs as well as utilized on multiple mobile platforms. It also efficiently works with Apples iPod touch and iPhone. This system is susceptible for location database manipulation. In this attacker as well as user can change the results of localization at targeted device, by either attacks may easily replicated. In safety-critical contexts WLAN based location should be referred. Author was further discussed about various strategies for securing WLAN-based positioning systems.

"S. Brands and D. Chaum,"Distance-Bounding Protocols, "discussed about location spoofing problems. Also they talked about exact co-ordinates location. It is provided by tracing required location. Hopping distance is cryptographic rules that were enabling authenticator to induct an upper bound on the physical distance. This technique is based on timing interruption between sending out challenge bits and receiving back the agreeing response bits. Time required to respond computes an upper-bound over the distance. The speed of light rays as the round trip delay time separated. This calculation is based on the fact of electro-magnetic waves that are travel nearly. But it cannot faster than electro-magnetic waves.

E."R. Khan, S. Zawoad, M. Haque, and R. Hasan,"OTIT: Towards secure provenance modeling for

 

location proofs," discussed about a framework. It is a model for designing secure location provenance. In this author normalized the personalities as well as some attributes required for domain of safe area origin. They used formal propositional logic as well as logical proofs. They are also introducing WORAL framework. Several schemes defined their own devotion for anticipated features of locations that are in safe locations.

## III. PROPOSED SYSTEM ARCHITECTURE

End user is having android app that has modules to part his placing details with the LV(Location Validator) also this app is having modules to produce placing provenance records and send it to the LV to support. Also user can manage his outline, and make an addition / report / take out the placing records is right for to him.

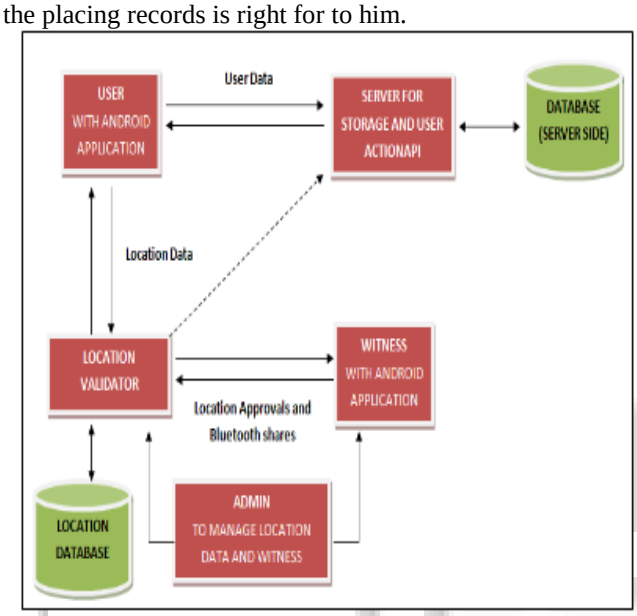


Fig. 1: System Architecture

Very first user, witness, Admin has to make come into existence an account on the SP. User has to make ready his nothing like it mind and physical qualities fact in support of for it. While recording, listing on the SP (Service Provider) each user has to make ready nothing like it username and password also to way in the facilities on condition that to the end user. While making come into existence an account of user, cryptographic-Id is used which is in number form and size and user 1 is taken to be with this cryptographic.

Administrator makes certain of the Witness and manage LV. It is must for this reason doing something can be kept out of after checking to make certain LV and witness can work with their parts.

SP is responsible to support right news between user and LV. This effect on one another is doted by having the same private and public keys. LV provides location-Id at times of account work of art and when LV is given authority then SP produces the private-public key-pair, which is taken to be by the location-ID. Last need to keep in order, under control the private key and store it on the nearby computer upon letting into one's house a request for the public key for one LV (location-ID),the SP sends the right public key to the user.

After frame for events these things in the framework we take into account the Case when user need to produce the placing fact in support of through the framework. User sends placing fact in support of request to the LV.

The LV produces the placing fact in support of LP (Location Proof). And meanwhile LV also sends the idea put forward request to the W (Witness) by putting to use random selection way on WL(Witness List).

One who saw makes certain of the idea put forward request and send put forward placing fact in support of High Mountain to LV.

LV sends High Mountain to the end user after right verification.

When end user gets LP , user directly exchange with the W. W gets the VReq from U(User) and checks to see if the idea put forward has been tampered or not. After good verification, W makes come into existence a verification statement Vs and send to the user. This can be done through Bluetooth share between user and witness W.

When user gets Vs from one who saw it send to LV to be stored as receipt for the idea put forward placing provenance and completed the approved design.

## IV. MATHEMATICAL MODEL

S = {s, e, x, y,Fn, DD, memsh}
Where,
s = Start State-Locate the location
e = End State-User Identification
Input:
x = Input State
x= {Ud,Wd,LAd,SPd}Here
x is input to the S.
Where,
Ud : User details require.
Ud is further divided as follows,
Ud = {Lreq,Rreq,CrId,Preq,LPR} Where,
Lreq : Login request
Rreq : Registration request
CrId : Crypto-id
Preq : Location proof request
LPR : Location Proof receipt
Wd : Witness details require.
Wd is further divided as follows:
Wd = {WLreq,WRreq,WCrId,ALP}Where,
WLreq : Witness Login request
WRreq : Witness registration request
WCrId : Witness crypto-Id
ALP : asserted location proof
LA={LALreq ,LARreq ,Lop} Where,
LALreq : LA Login request
LARreq : LA registration request
Lop: Location proof
SPd : Service provider details
Output:
y = Output State
Op = {WLop , LocList , PrGen , LPr} Where,
WLop : Witness List
LocList : Location List
PrGen : Location Proof Generation Message
Lpr : Location proof trails of user
Functions: Fn is function
Fn = {LogF , RegF , CrIdGenF , AssertMsgF , ValidateMsgF , getLat LongF} Where,

 

LogF : Login function for User ,
LA and witness
RegF : registration function for User , LA and witness
CrIdGenF : Crypto-Id generation function
AssertMsgF : Location Assertion Message Generation Function
ValidateMsgF: Validate requests from user and witness functions
getLatLongF : Get Latitude and longitude

- Success Conditions: Witness Present at the location can check the location proof
- Failure Conditions: If witness not present can check the witness location proof.

## V. Analysis and Results

It is analyzed that user has to register first. User cannot share data about location if his shared location is not validated by witness. When user want to share data about particular location then his existing locations are populated and verified by witness through Bluetooth sharing. After location verification user can add destination details. User can get / download the details about location by proxy or original location sharing.
Following are the details of Implementation :
Following is the home screen having options to deal with the system

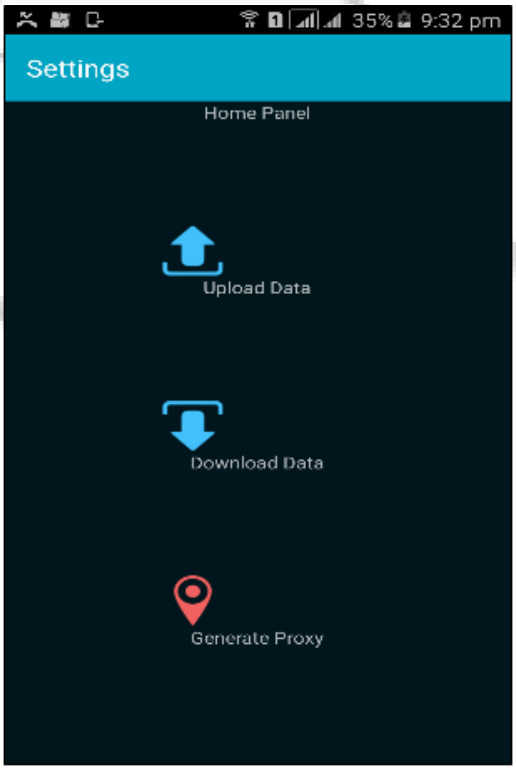


Fig. 2: Screen1

Screen 2:

Following is the screen that help user to upload data. At the back end user latitude and longitudes are fetched and location is verified automatically through witness.

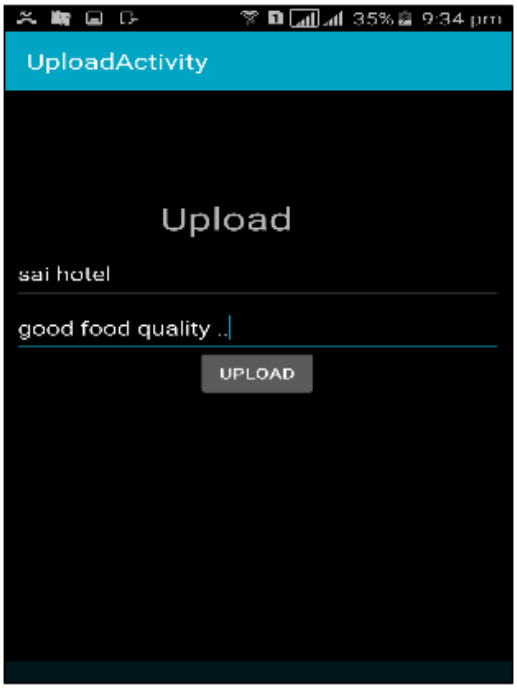


Fig. 3: Screen2

Following is the screen that help user to generate his proxy location to get details about that location.
Screen 3:

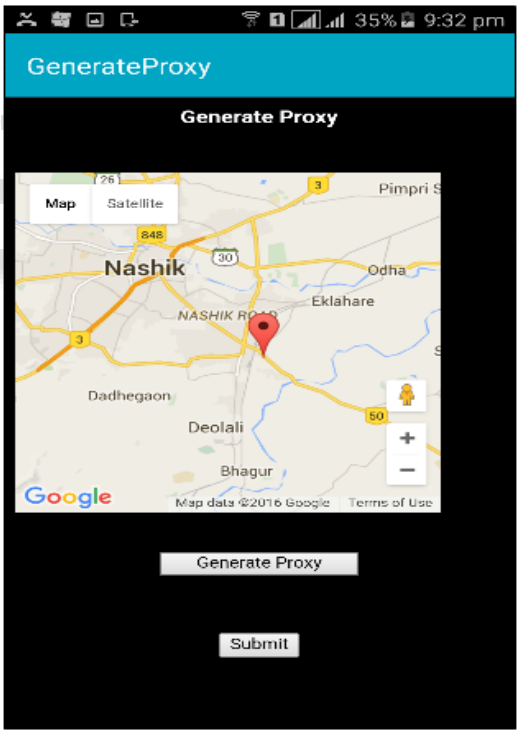


Fig. 4: Screen4

## VI. Conclusion

In this paper we proposed a system to preserve privacy of user as far as identity and location. Our system also provides location verification effectively. With our system, this location verification process has to be done automatically with minimum chances of manipulation. Hence proposed protocol has to deal with mentioned crisis effectively. This protocol help user to maintain his location visit trails on server and system administrator as well as user can access his location visits along with verification proofs. Also user

 

will get recommendation of his friends available in that area. This is add on feature added which will be useful for the end user.

## REFERENCES

[1] S. Saroiu and A. Wolman,"Enabling new mobile applications with location proofs," in Proc. of HotMobile, 2009
[2] I.Maduako, "Wanna hack a drone? possible with geolocation spoofing!",July 2012.
[3] N. O. Tippenhauer, K. B. Rasmussen, C. Popper, and S. Capkun, "iPhone and iPod location spoofing: Attacks on publicWLAN-based positioning systems," SysSec Tech. Rep., ETH Zurich, April, 2008.
[4] S. Brands and D. Chaum,"Distance-bounding protocols," in Proc. of EUROCRYPT Springer-Verlag New York, Inc, 1994
[5] R. Khan, S. Zawoad, M. Haque, and R. Hasan, "OTIT: Towards secure provenance modeling for location proofs," in Proc. of ASIACCS. ACM, 2014.
[6] www.roseindia.com
[7] www.w3schools.com.

 