IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 30-35
www.iosrjournals.org

User Location Provenance Witness And Proxy Generation Framework.

Jadhav Pallavi S.[1], Khalkar Supriya S.[2], Randhavane Sonali B.[3] ,Joshi Sunil R.[4]
Singh Seema A.[5]
[1,2,3,4,5](Dept. of Computer Engineering ,KVNNIEER Nasik ,SPPUniv.Pune(MS), India)

***Abstract**: During the last few years, usage of mobile phones as an authorized work and various institutes use mobile devices as an expert communication. Location based services allow users to provide a physical location provenance proof and privacy protection. Our framework maintains a privacy of data sharing and provides witness proof. It is a significant challenge to generate provenance witness and generate a proxy in one fabric. So far propose system accomplish the framework requirement. We are producing a different framework for location specific secure data sharing, which will afford user location proofs generation and proxy location. It is ready-to- deploy framework for secure, witness-oriented, and provenance preserving location proofs.*

***Keywords:** Location assertion, Location provenance, Location Security, Witness, Proxy generation, WORAL.*

I. Introduction

Geo-social networking is the new inclination of social media networking. People always beliefs on other people about their location providence even when they have access to huge quantity of data, such as the internet and location witness amenities. Now in social networking geosocial network works with a location provenance and data shared by different users and this information can be used by other users to acquire significant data about several dissimilar places and things. Best examples of geosocial networking are friend locator, location based recommendation, etc. Since these applications make use of location provenance of the user trade places and used as a witness services. These applications have a huge number of users due to that it needs stronger privacy setting than the open source applications. Today, many administrations are demanding to use location provenance application as a witness proof in their market amenities such as product delivery services.

Mobile devices have increased the use of location based amenities using the geographical position of devices. But due to deficiency of security, they are unsuccessful to apply location provenance application as a corporate use. So they need more detailed network application built on location provenance witness services. There have been a number of applications for permitting user specific location proof generation. A location authority covering the range exploits some secure distance bounding mechanism to support the user's existence when the user demand for a location proof.

A rapid estimation in information technology and wireless communication. Now a day it is rattling essential for everybody to be informed about recent activities such mobile phones, news, stock markets. Concern as well as customer products are progressively gearing towards flexibility and location based amenities. This is where our study concentrations on the facility of mobile devices which provides software solution which are location sensitive. As per whole discussion we need to implement location based services with the support of application based which can be beneficial to apply on business and can monitor with witness proof, so we have to establish a secure framework which will accomplish requirement of the user with proxy option also. We provide an advanced framework for location precise, secure data sharing which offers integrative amenities of user location proofs generation and proxy location. We have proposed new technique for providing enhanced security to the user statistics and uploaded information on the server, this technique is cryptography. In cryptography the encryption and decryption algorithms are used to afford security and match public keys, to hide the significant information of the user and location. For location provenance proofs and assertion we have established new framework and the proxy generation concept is summed in this framework for preserving location privacy. Our objective is to support both queries. It is suitable for the latest mobile devices. It provides future flexibility to support circular range, level, nearest queries on location information. We afford robust location privacy by using encryption, decryption algorithms.

II. Literature Survey

Persons have proposed liability contrivances to discourse privacy concerns of end users and then improve a privacy manager. The notion is that the user's private records are sent to the cloud there that will transform into an encrypted form of data, and the dispensation is completed on the encrypted data. The yield of the procedure is data which is in a decrypted format by the privacy manager to discover the accurate outcome if that precise further user or friend enters that key. Though, the confidentiality manager offers only limited scenery in that it does not assurance defense once the data are being revealed. [1]

The key factor of location privacy discriminates permitting to the information processing and chronological placement. These accomplishments are contained, gathering of data; conservation or inappropriate storage; use of data; disclosure of location related information. Certain recommended systems used in the previous years to overwhelm the location privacy coercions such as spatial k-anonymity, fake location, cloaking/obfuscation, cryptographic, Trusted third party protocol (TTP), simple and multiple pseudonym, semi distributed protocol, Private Information Retrieval protocol (PIR), collaborative protocol, and user centric. [1]

Location coordinates mention to the longitude, latitude pairs associated with real-world positions. A pair of coordinates is reimbursed from a GPS, and is employed to tie in information with a placement. Location data or location information refers to such data linked to a location. We have reviewed the papers and study the papers. In this paper, we develop witness oriented architecture for producing secure location proofs. [1]

The strategy and cognitive process of an innovative P2P data sharing protocol, called OneSwarm that delivers users more enhanced secrecy than Bit Torrent and much better concert than Tor or Freenet. An important feature of the OneSwarm design is that users have clear configurable mechanism over the expanse of conviction they place in peers and in the distribution model for their data: the identical statistics can be shared freely, secretly, or with access mechanism, with both reliable and untrusted peers. [2] Through a discrete encoded identifier vocabulary with hashed and authentic values of all exclusive collections of identifiers, we recommend re-designation of any data dispensation outcomes. We recommend a methodology to accomplish data safety & privacy all over the complete data lifecycle: data generation/gathering, transmission, storage, dispensing and distribution. [3] A system for privacy preserving subcontracted mining and presentation that the marketer can improve the true outlines as well as their provision by maintaining a compressed outline. [5]

Location-based amenities mobile applications are fetching progressively dominant to the vast population of semi-literate users living in evolving frugalities due to the low budgets and ubiquity. Still, utilization of location-based amenities is still susceptible by information privacy trepidations. Studies typically only addressed how to moderate information privacy trepidations for the literate users and not the semi-literate users. To fill that gap and well known information privacy trepidations among different groups, this study draws upon concepts of perceptual control and awareness to recognize the backgrounds of information privacy trepidations related to location-based services and user mastery. [7] Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices. Privacy-preserving algorithms for defining an optimum meeting location for a crowd of users. We accomplish thorough privacy estimation by correctly enumerating privacy-loss of the proposed approaches.

III. Modeling The Woral Framework

In this section, we describe the models and terminologies for developing the user specific location, provenance proofs and proxy generation framework. In this context we define security as ensuring the integrity and privacy for viewing location, provenance witness to a particular user or all site users.

3.1 Terminologies

We have produced certain terminologies in the implementation of our models and for designing the protocol architecture. A user U is an entity who visits a special location and user a mobile application to show their position. A site S is a physical region, which provided to the user to visit and generate location witness proofs. The service provider SP is the trusted entity which provides the secured location, provenance to application mobile user. A location authority LA is a stationary entity authorized by the service provider SP, which identified by a unique identifier, and it is response for providing location witness proof for the particular physical area. A witness W is a location co-ordinate of users who visited the particular physical area and provided by GPS through mobile devices. A cryptoId CID is a cryptographic identify for application user (who is likewise a spectator). A location proof LP is a witness's evidence received by application user who visiting the specific physical area. Asserted proof AP is a location proof. The auditor is an SP verify authority who will generate authenticate witness proof and validate witness proof is correct or not. **Proxy generation PG** is trusted entity which will ensure that provided witness (which provided by user) is correct proof or not with the help of location proxy generation of the particular physical area region.

3.2 Threat Model

The threat model design for user specific location, provenance proofs and the proxy generation framework is based on the terminologies describes as follows: The position data within the asserted location, witness proof corresponds to the watcher of a user and an entity which cannot be able to create a location witness which that the user has hotly visited. The time at which the user U visited the special position and collected the asserted location proof should not be modifiable by an attacker to make a witness proof for a different time than the actual visited time of that placement. The user can provide a security to who can view witness proof of location.

3.3 System Model

We assume that mobile devices carried by users are android base operating system with GPS services and capable of communicating with other devices, over a service provider network. The devices take in local memory for storing the provenance item. The user has total access to the storage and computation of the device, can install an application on the device and can modify insert and edit content in the data. The user LA and witness can access each other's public key from the SP.

IV. System Architecture

Five entities are involved in the propose framework: The application mobile device users, The LA, auditor, The SP and proxy generation (PG). In the secure asserted location, province protocol, a user U visit a particular site S, which is defended by an LA. There are a number of devices produces a witness proof W. Which will verify by an auditor. The SP is the only centralized entity in the proposed architecture, which is responsible to handle the different explanations of the application user provide authentication, and dispute public keys, figure 1 depicts the overview of the proposed architecture. The communication between location authority (LA) and mobile users are done over TCP. Whole messages are signed and coded using the secret key of the respective entities and verify using the public key. Signature of an entity of a message M is we are referring as $S_{E(M)}$. An entity from the SP. All communication with the SP occur through the public network using REST[1] and HTTPS.

The various different stapes and phases of protocol have been design, to ensure the locaton proof is resistent to collusion attack and provenance of the location proofs is preserved. Proxy generation communication with SP and retrive witness proof and generate proxy for provided co ordinates for each location as user visits they will generate witness proof for every location. After generating proxy of retrieved co-ordinates and validate provided location proofs is valid or not.

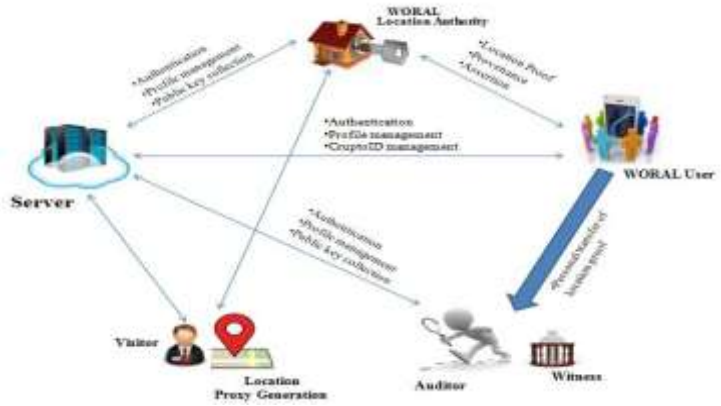

Fig 1:System Architecture

4.1 Secure Location Provenance Protocol & Proxy Generation

a) Location proof request The user obtains the identity of the LA and sends a location proof request PReq to the LA, as shown in Expression 1.

Req = < CIDU; tU; PS; LProvcur; SL(CIDU; tU; PS; LProvcur) > (1)

b) Location proof generation The LA generates the location proof LP as shown in Expression 2 and sends the LP to the user.

LP = < CIDU; L; tL; LProvnew; SL (CIDU; L; tL; LProvnew) > (2)

c) Proof assertion request The LA randomly selects a witness W from the WL and then sends an assertion request AReq to the selected W, where AReq = LP.

d) Asserted message creation

The witness W verifies the information in the AReq message. Upon successful verification of all the information, the asserted location proof ALP, as shown in Expression3, is sent to the LA.

ALP = < LP;CIDW;CIDU; L; h(LP); tW; SW(CIDW;CIDU; L; h(LP); tW) > (3)

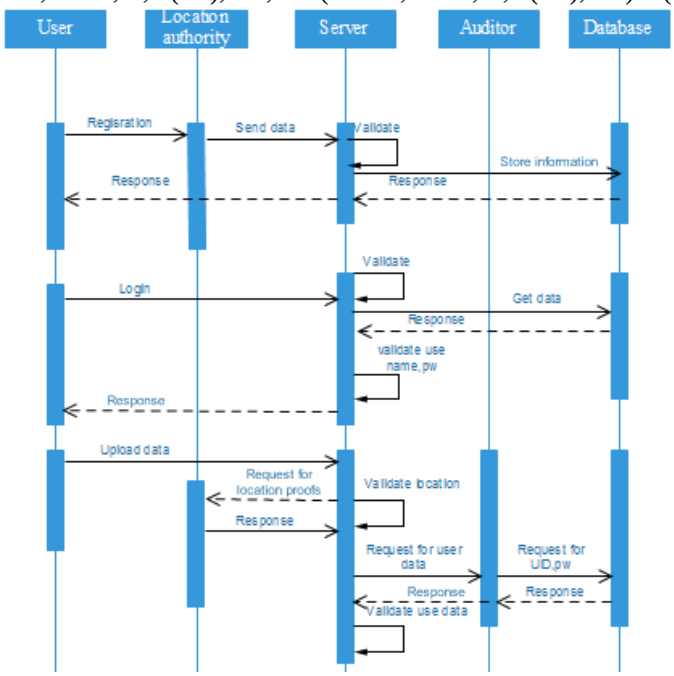

Fig 2: Sequence Diagram For User

e) Assertion verification and relay

The LA receives and verifies the ALP for the assertion provided by the W. The LA also verifies the time lapse between sending an assertion request AReq and receiving the asserted location proof ALP, i.e., difference between tL available from ALP, and the current time at the LA. This time difference is referred as TLW in Figure. The LA enforces a maximum threshold for the TLw to detect any proxy forwarding delay by the witness. The process of identifying the appropriate value for the TLw is presented. Upon successful verification, the LA relays the ALP to the user U.

f) Verification request

Once U has received both the LP and the ALP; he directly communicates with W, and sends a verification request VReq, as shown in following Expression.

VReq = < ALP; LP; h (ALP; LP); tu > (4)

g) Verification response

W receives the VReq from U and checks to see if the assertion has been tampered or not. W calculates the difference between the time tw, available in the ALP, with the current time on the witness device. This time difference is referred as Twu in Figure. A Maximum acceptable value for the Twu ensures that U is not trying to collect the ALP through a proxy. After successful verification, W creates a verification statement VS, as shown in Expression, and sends it to the user U. Twu is the response timestamp for the Ws verification.

S= < R; t_{WV} ; SW(R; t_{WV}) > R2[Y ES;NO](5)

h) Location proof receipt

After receiving the VS from W, the user verifies the time difference between the time in the V Req tu and the current time on the users device when it receives VS. In Figure 3, this time difference is referred as Tuw. A maximum threshold for the Tuw, ensures that W is not proxying the assertion and the verification requests. U then creates an acknowledgement ALPAck as follows:

AS = < LP;CID_W;CID_U; L; h(LP); t_W >

(ALPAck = < S_U (LP; AS); h (LP; AS); t_T > :(6)

I) Location Proxy Generation: After receiving ALP from client user, after a visitor will generate proxy obtained by user witness proof for particular users location coordinates.

PG_{gen}=<ALP (x, y→x', y')... (7)

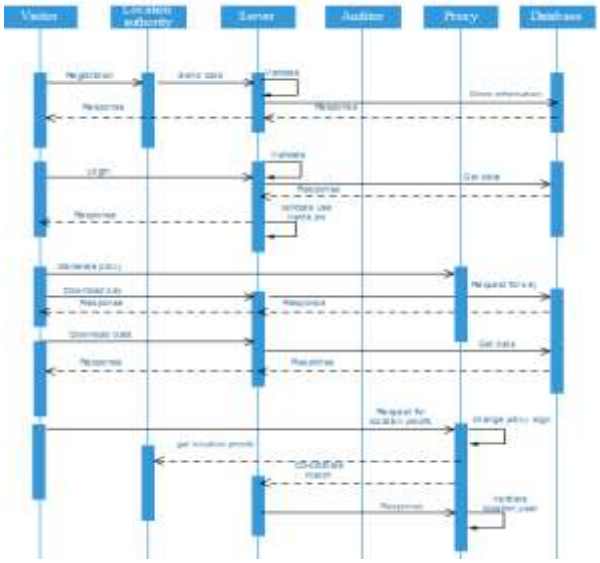

Fig 3: Sequence Diagram for Visitor

V. Conclusion

Collection and verification of location proofs have significant real life application in location based services. We work on secure location provenance chains to allow auditors to validate user's presence of different locations. It provides the location proof efficiently and preserves the location privacy with collusion resistant. The paper presents the schematic development, feasibility of usage, comparative advantage over similar protocols, and implementation of WORAL for Android device users for enhanced usability.

VI. Future Scope

The project ensuring distributed data sharing and security in android & cloud is to. After uploading data on cloud this project will maintain all the records about user who have used the data. Also bundling of the file with its information and accessing that data or location by getting that particular key & through that we can preserve our location is the scope of the system. Users can obtain multiple Crypto-IDs from the SP, which ensures privacy by creating a many-to-one mapping of the Crypto-IDs to the original identity. Our current research includes temporal-anonymizing of the identity for the users. In this new scheme, all interactions among each other at different sites will be based on a temporal identity created by the user on run time.

References

[1]. Antorweep Chakravorty, Tomasz Wlodarczyk, Chunming Rong, "Privacy-Preserving P2P Data Sharing with OneSwarm" SIGCOMM'10, August 30–September 3, 2010.
[2]. Antorweep Chakravorty, Tomasz Wlodarczyk, Chunming Rong, "Privacy Preserving Data Analytics for Smart Homes" Department of Computer & Electrical Engineering, 2013.
[3]. Larry A. Dunning, Member, IEEE, and RayKresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment" Department of Computer Science, Bowling Green State University, 2013.
[4]. Fosca Giannotti, Laks V. S. Lakshmanan, Anna Monreale, Dino Pedreschi, and Hui (Wendy) Wang, "Privacy Preserving Mining of Association Rules From Outsourced Transaction Databases" University of British Columbia, Vancouver, Canada, 2013.
[5]. Stanislav Mamonov &Raquel Benbunan-Fich, " Factors Affecting Perceptions of Privacy Breach among Smartphone Application Users" 2014 47th Hawaii International Conference on System Science.
[6]. Adrian Z.Y. Tan, Wen Yong Chua &Klarissa T.T. Chang, "Location Based Services and Information Privacy Concerns among Literate and Semi-Literate Users", 2014 47th Hawaii International Conference on System Science.
[7]. Igor Bilogrevic, Murtuza Jadliwala, Vishal Joneja, " Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices" IEEE Transactions On Information Forensics And Security, Vol. 9, No. 7, July 2014.

[8]. Krishna P. N.Puttaswamy Shiyuan Wang, Troy Steinbauer, Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel and Ben Y. Zhao, "Preserving Location Privacy in Geo-Social Applications" Department of Computer Science, 2014.
[9]. Qinghai Liu, Hong Shen and Yingpeng Sang, "Privacy-Preserving Data Publishing for Multiple Numerical Sensitive Attributes" June 2015.
[10]. Ragib Hasan, Rasib Khan, Shams Zawoad, and Md Munirul Haque, "WORAL: A Witness Oriented Secure Location Provenance Framework for Mobile Devices" IEEE Transactions on Emerging Topics in Computing, 2015.