User Specific Location Provenance Proofs and Proxy Generation Framework

Joshi Sunil R.¹ JadHAV Pallavi S.² Randhavane Sonali B.³ Randhavane Sonali B.¹ Prof. Singh Seema A.⁵

1,2,3,4,5 K.V.N.Naik Institute of Engineering, Education & Research, Nashik

Abstract— During last few years, use of mobile phones as a official work and many organization using mobile device as a business communication. Location based services allow user to provide physical location provenance proof and privacy protected. 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 framework so far propose system fulfill the framework requirement. We produce a novel framework for location specific secure data sharing which will provide user location proofs generation and proxy location.

Key words: Location assertion, Location provenance, Location Security, Witness, Proxy generation, WORAL

I. INTRODUCTION

Geosocial networking is now new trend of social media networking people always trust on other people about their location provenance even when they have access to large amount of information such as the internet and location witness services. 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 get important data about various different places and things. Best example of geosocial networking are friend locator, location based recommendation since these application make use of location provenance of the users locate places and used as a witness services. These applications have large number of users due to that it need more stronger privacy setting than the open source applications. Today many organizations are trying to use location provenance application as a witness proof in their market services such as product delivery services.

Mobile devices have increased the use of location based services using the geographical location of devices. But due to lack of security reasons they are failed to apply location provenance application as a business use. So they need more precise network application based on location provenance witness services. There has been more number of proposals for allowing user specific location proof generation. A location authority covering the area utilizes some secure distance bounding mechanism to ensure the users presence when the user request for a location proof.

The following example illustrates the practically of secure and asserted location provenance framework. John is an engineer at a construction company. The company requires John to travel and visit the construction sites create a daily basis report of the site project status. Unfortunately, John is charged with negligence towards his job when the company suffered a major loss due to an accident. The inspection report by seniors that John presented was discarded for being a fake document as the company claimed that John did not visit the site and the accident was a result of his negligence. In an alternate scenario, John will collect location provenance records as he visits each of the construction sites, which are asserted by the application as a witness. Therefore, John can then prove his regular visits and the order of visit to each of the sites based on the more secure location provenance records.

A rapid evaluation in information technology and wireless communication. Now a day it is very necessary for everyone to be update about current affairs such mobile phones, news, stock markets. Corporate as well as consumer products are increasingly gear towards mobility and location based services. This is wherever our study focuses on the flexibility of mobile devices which provides software solution which are location sensitive. Location based mostly services area unit unit data and recreation services accessible with mobile devices through mobile network and utilizing the flexibility to create use of geographical position of the mobile device. Mobile devices send and receive radio signals with any number of cell site base stations. As smart phones and tablets become more popular. The operating systems for those devices become more important.

II. RELATED WORK

Persons have proposed accountability mechanisms to address privacy concerns of end users and then develop a privacy manager. The concept is that the user’s private information is sent to the cloud there that will converted in an encryption form of data, and the processing is done on the encrypted data. The output of the process is data which is in decrypted format by the privacy manager to reveal the proper result if that particular other user or friend enters that key. However, the privacy manager provides solely restricted options in that it does not guarantee protection once the data are being disclosed.

The major component of location privacy differentiates according to the information processing and temporal sequence. These activities area unit together with, collection of data; retention or improper storage; use of data; revelation of location associated info. a number of the steered techniques used in the last few decades to overcome the location privacy threats like special k-anonymity, dummy location, cloaking/orfuscation, cryptographic, Trusted third party protocol (TTP), straightforward and multiple anonym, semi distributed protocol, Private Information Retrieval protocol (PIR), collaborative protocol, and user centric.

Location coordinates refer to the longitude, latitude pairs associated with real-world locations. A pair of coordinates is returned from a GPS, and is used to associate data with a location. Location knowledge or location info refers to such knowledge associated with a location. We have reviewed the papers and study the papers. In this paper witness oriented architecture for generating secure location proofs.
III. SYSTEM ARCHITECTURE

Location based services for mobile devices have more popular in recent times authentication, authorization, access information, data privacy, proxy generation, location proof generation and similar critical actions can be associated with geographical locations of the devices. The location information is used by server to provide location details of the user. The system provides extra level of security by getting the enunciation of proof from witness. There are four entities involve in this architecture Users, Location authority, Service provider (Server), auditor. In the secure asserted location provenance protocol, a user visits a site S, which is maintained by a Location authority. The service provider is centralizing entity in this architecture which is responsible to manage accounts of other three entities, provide authentication, public key collection, and profile management.

In this framework, users, witnesses, Location authorities, and auditors need to create an account with the Service provider using unique identification criteria. As the Location authority and auditor needs to be licensed entities, there's associate account verification stage for these two entities. The Service provider verifies the Location authority and auditor account requests and sends them a service code. LAs and auditors cannot access their accounts till the accounts are activated using the service code received from the SP.

![System Architecture Diagram](image)

The User is directly communicated with net interface or service supplier, profile management, public key collection, crypto ID management. At the time of authentication the users are under observation of auditor means auditor audit the proofs. Also matching public keys, profile management & authentication. An Auditor is an SP verified authority who is presented with a chain of declared location proofs and confirms the legitimacy of the user’s claim of presence at the particular site and the order of visits. The auditor is a standalone Java desktop application communicating with the service provider. The user presents associate exported proof (or list of proofs) and the auditor imports the file to verify the location proofs and their cradle. Two of the panels from the auditor window, for the LA provided information and for the witness assertion.

IV. OBJECTIVE OF GIVEN FRAMEWORK

A. Strong Location Privacy

The servers processing the data (and the administrators of these servers) should not be able to learn the history of location that a user has visited.

B. Location Proofs

As now many organizations are dependent on location proofs. so we trying to solve the problem related to witness proofs. And with the help of WORAL framework solving derived problems.

C. Proxy Generation

A new framework is generated with the help of concept proxy generation. With the help of proxy generation a visitor of our system without visiting at particular location can be audit the witness proof.

D. Location Provenance

As now a day’s various organizations required the location provenance (specific location) for better evaluation of workplan. so the system will provide exact location provenance to user.

E. Location Security

Due to various users working and interacting with system, there are various chances to lost location security. We develop a new idea to generate privacy to particular user or all site users.

V. FUTURE WORK

The project guaranteeing distributed information sharing and security in android & cloud is to. After uploading data on cloud this project can maintain all the records concerning user World Health Organization have used the data. Also bundling of the file with its information and accessing that information or location by obtaining that specific 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 initial identity. Our current research includes temporal-anonymizing of the identity for the users. In this new theme, all interactions among each other at different sites will be based on a temporal identity created by the user on run time.

VI. CONCLUSION

Collection and verification of location proofs have vital real life application in location based services. We work on secure location provenance chains to permit 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, practicability of usage, comparative advantage over similar protocols, and implementation of WORAL for Android device users for enhanced usability.

ACKNOWLEDGMENT

The authors would like to thanks to the researchers and publishers for making their resources available and teachers
for steeraage. we tend to conjointly convey to authority for supporting to us and providing required information.

REFERENCES


