International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 04 | April -2020 ISSN: 2582-3930

A Privacy-Preserving Location proof Updating System (APPLAUS)

RENUGA DEVI S

Assistant professor Mr. K. NIRMAL

Krishnasamy College of Engineering and Technology,
Cuddalore

Abstract: Today's location-sensitive service relies on user's mobile device to determine its location and send the location to the application. This approach allows the user to cheat by having his device transmit a fake location, which might enable the user to access a restricted resource erroneously or provide bogus alibis. To address this issue, we propose A Privacy-Preserving Location proof Updating System (APPLAUS) in which co-located Bluetooth or WIFI enabled mobile devices mutually generate location proofs, and update to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. We also develop user-centric location privacy model in which individual users evaluate their location privacy levels in real-time and decide whether and when to accept a location proof exchange request based on their location privacy levels. APPLAUS can be implemented with the existing network infrastructure and the current mobile devices, and can be easily deployed in Bluetooth or WIFI enabled mobile devices with little computation or power cost. Extensive experimental results show that our scheme, besides providing location proofs effectively, can significantly preserve the source location privacy.

1.Introduction: Mobile devices, such as smart phones and PDAs, are playing an increasingly important role in people's lives. Location based services take advantage of user location information and provides mobile users with a unique style of resource and services. Nowadays more and more location-based applications and services require users to prove their locations at a particular time. As location proof plays a critical role in enabling these applications, they are location-sensitive. The common theme across all these applications is that they offer a reward or benefit to users located in a certain geographical location. Thus, users have the incentive to lie about their locations.

There are many kinds of location-sensitive applications. One category is location-based access control. Meanwhile, one class of popular location-aware applications works only when users are able to prove their history locations, such as auto insurance quote in which auto insurance company might provide discounts to drivers who can prove that they take high-safety routes during their daily commutes, fraud reduction on eBay in which location proofs from the seller can serve as additional evidence that the seller's account has not been compromised by an attacker police investigations in which police forces are interested in finding ways for people to be able to provide efficient and trusted alibis, and location-based social networking in which a user can ask for a location proof from the service requester and accepts the request only if the sender is able to present a valid location proof.

2.EXISTING SYSTEM: Submit the location proof directly. Can't send location proof automatically. Only find the mobile using GPS emulator. Device is requiring finding current location.

3.PROPOSED SYSTEM:

Small-footprint application does not interfere with any phone operation. Secure Web portal for locating your phone. User control for suspending(and resuming)tracking. Accurately locates your phone to within same distance. Location proof sends through your android mobile. Don't require any device to find the location.

4.SYSTEM ARCHITECTURE:

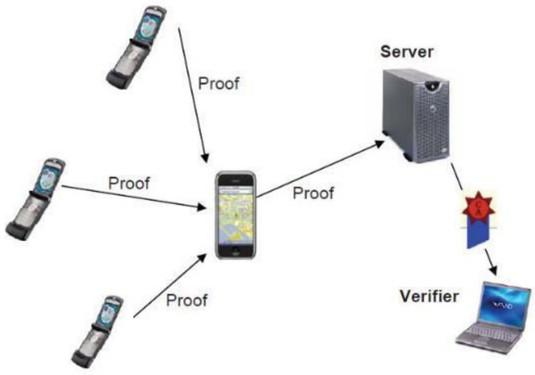


Fig.1 System architecture

5.MODULES:

- Location Based Service
- Location Proof
- Location Privacy
- Pseudonym
- Colluding Attacks

5.1.LOCATION BASED SERVICE:

GPS Tracking utilizes your phone's internal GPS hardware to obtain an accurate reading of the location and transmit it .This applications allows you sharing your GPS location. Allow Android device users to share their exact location by way:

- Readable address:

  Readable address is a simple tool that can help you find the

  approximate address of any point with Area code, Street Name, Nearby Location.

- Google Map Link:

  Locate where your Android device is in real time using a high resolution map viewable on any web browser.

5.2 LOCATION PROOF: As our goal is not only to monitor real-time locations, but also to retrieve history location proof information when needed, a location proof server is necessary for storing the history records of the location proofs. It communicates directly with prove nodes who submit their location proofs. As the source identities of the location proofs are stored as pseudonyms, the location proof server is untrusted in the sense that even though it is compromised and monitored by attackers, it is impossible for the attacker to reveal the real source of the location proof.

5.3 LOCATION PRIVACY: Now we look at how an adversary may reveal location information by analyzing the location proof history. Suppose the attacker has sufficient resources (e.g., in storage, computation and communication).

First, the attacker may simply monitor content of a record that may contain the user’s identity and location. Second, even if the user’s ID is encrypted or pseudonymized, it is easy for the adversary to trace back all the location activities related to the same ID once its pseudonym is discovered. Third, even though the user’s pseudonyms change periodically, it is still possible for the adversary to infer this user’s other pseudonyms from one pseudonym if these pseudonyms change at similar time or locations.

Moreover, the attacker may perform more advanced traffic analysis including rate monitoring and location correlation. In a rate monitoring attack, the attacker tries to monitor and correlate location proof updating rates from different pseudonyms. In a location correlation attack, the attacker may observe the correlation in updated location between a node and its neighbor, attempting to deduce a relationship.

5.4 PSEUDONYM: A pseudonym is a name that a person or group assumes for a particular purpose, which differs from his or her original or true name (orthonym). Pseudonyms include stage names, screen names, pen names, nicknames, aliases, gamer identifications, and reign names of emperors, popes and other monarchs. taken the form of anagrams, Graecisms, and Latinisations, although there are many other methods of choosing a pseudonym. Pseudonyms are most usually adopted to hide an individual's real identity, as with writers' pen names, graffiti artists' tags, resistance fighters' or terrorists' norms de guerre, and computer hackers' handles. Actors, musicians, and other performers sometimes use stage names, for example, to mask their ethnic backgrounds.

Employers sometimes require employees to use assigned names to help sell products: for example, a company that does business mostly in one country but locates a call center in another country may require its employees to assume names common in the former country to try to draw a more positive or less negative reaction from current and/or prospective customers.

5.5 COLLUDING ATTACKS:

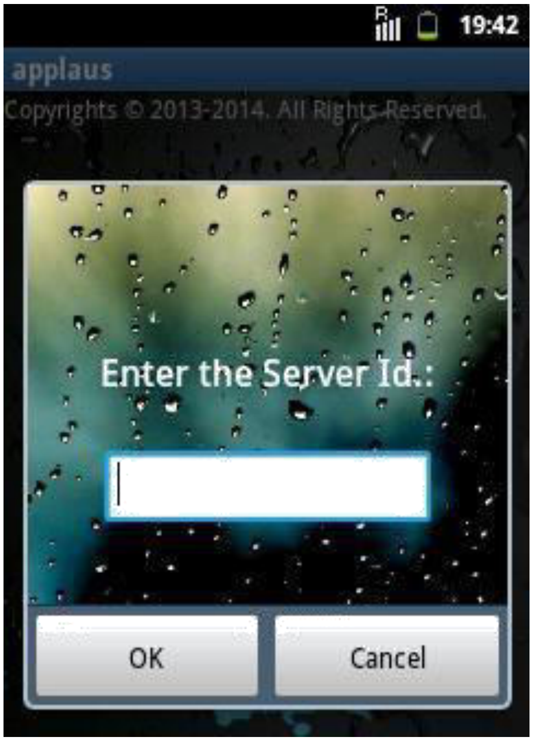
The collusion attack is an action carried out by a given set of malicious users in possession of a copy of protected content that join together in order to obtain at the end of the attack procedure an unprotected asset. The attack is carried out by properly combining the protected copies of the multimedia documents collected by the colluders, according to the type of content and the kind of adopted protection system.

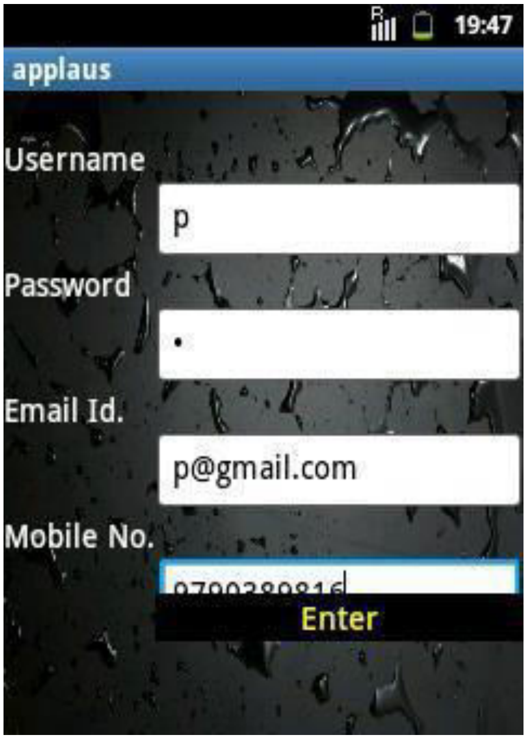
EVALUATION:

APPLAUS NETWORK IN SOCIAL FIELD:

APPLAUS server in the network, users can make use of its services on a primary level was registered. In response, the server, the user ID of a user. Each mobile node in the network before entering the public/ private key pairs, which is composed of a set. The user back to the server at the end of the Bluetooth device name and device ID are stored. After the user is logged in to a friendship, and he

finds the name of the new users will be forwarded to the social network. He requested that his account of the user's request will be presented to the user with a third party. Deny the request to the third-party user in the network, and can accept a friendship.





Username p

Password •

Email Id. p@gmail.com

Mobile No. 07900380816

Fig.3 User Registration

APPLAUS APK

CONCLUSION: This project proposed a privacy-preserving location proof updating system, called APPLAUS, in which co-located Bluetooth enabled mobile devices mutually generate location proofs, and upload to the location proof server. We use statistically changed pseudonyms for each device to protect source location privacy from each other, and from the untrusted location proof server. We also develop user-centric location privacy model in which individual users evaluate their location privacy levels in real-time and decide whether and when to accept a location proof exchange request based on their location privacy levels. To the best of our knowledge, this is the first work to address the joint problem of location proof and location privacy. Extensive experimental and simulation results show that our scheme can provide location proofs effectively while preserving the source location privacy at the same time.

FUTURE ENHANCEMENTS:

Using location update system gathers the all related information about the citizen. That information uploads and update directly from the location. This project used to update the location where we are now and upload the picture of location proof. This is used to passport enquiry and address proof verification.

REFERENCES:

[1] Location Based Services on Mobile in India For IAMAI - Version: 14 April 2008.

[2] Location Management for Mobile Devices Erik Wilde (School of Information, UC Berkeley)-February 2008.

[3]Android Wireless Application Development By Shane Condor and Lauren Darcy.

[4]XianhuaShu “Research on Mobile Location Service Design Based on Android”, Wireless Communications, Networking and Mobile Computing, 2009.

[5]A.R.Beresford and F.Stajano, “Location Privacy in Pervasive Computing,” IEEE Security and Privacy, 2003.