UGC Approved Journal

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 8, August 2017

STAMP: Enabling Privacy Conserving Location Evidences for Cellular Users

Shimpleshwari[1], Prof. Vivekanandreddy[2]

PG Scholar, Computer Science and Engineering, Visvesvaraya Technological University, Belagavi, India[1]

Faculty, Computer Science and Engineering, Visvesvaraya Technological University, Belagavi, India[2]

Abstract: In this real world, location-based utilities are becoming immensely prominent. These offerings primarily depend on users' present location and also on history of users location. Without carefully designed safety system for web consumers, malicious or harmful users may lie about their spatial temporal provenance to show their past locations. The data can be faked and can be distorted for meeting particular prerequisites. Location dependent offerings need the user to provide location evidence at a particular time in use. There are a few cases wherein consumers may cheat on their locations. So here, one secure approach called Spatial-Temporal provenance assurance with Mutual Proofs (STAMP) for web application users is introduced. STAMP is designed for web users producing masked evidence for every different in a allotted setting. Anyhow, it can easily accommodate trusted web users and privacy for web consumer by generating mask id so this ensures the trustworthiness and non-transferability of the location evidences and make safe for user's privateness. Prototype implementation of this android application depicts that it is less expensive in phrases of estimation and system resources.

Keywords: Location evidences, privacy, trustworthiness, spatial-temporal provenance.

I. INTRODUCTION

Almost the present location-dependent utilities for web consumers are based on users' present web location. Web consumers discover their locations and share them with a server by doing the check-In Process. In turn, the server performs computation based on the region details and returns data/services to the web consumers. This leads to a wide variety of new location-evidence dependent Web applications. In our proposed method, once the web user is register on STAMP web application, in prover web server cryptography encrypted and user id will be generated based on their user id .This cryptography user id cannot be view by malicious user. Every time user access web application their cryptographic id will be matching for existing user are not if not user has to register with stamp application. Once user is register using user id they doing check in process to write a comment on that quality and service (implemented to Restaurants).Once this done with check in process for the user id, prover server will generate masked using that they can get the privacy while writing the reviews and giving rating on that restaurants and their number of visiting count will be counted every time they do check in process. By checking the fake user review location and the web user privacy details stamp application has better application while comparing to earlier system.

Online interpersonal organizations have become significant source of individual details. In Existing System, users voluntarily reveal a wealth of personal data, including age, gender, contact information, preferences and status updates. A recent addition to this space, geosocial networks (GSNs) such as Yelp and Foursquare further collect fine grained location information, through check-ins performed by users at visited venues. Personal information allows GSN providers to offer a variety of applications, including personalized recommendations and targeted advertising, and venue owners to promote their businesses through spatio-temporal incentives, e.g., rewarding frequent customers through accumulated badges. Determine their location, e.g., using GPS. However, it allows malicious users to fake their STP information. This leads to some disadvantages such as personal details exposes however consumers to significant risks and very less Network Security for Web consumers.

II. RELATED WORK

Recently, several systems have been proposed to provide end users the ability to provide that they were in a particular place at a particular time. Saroiu et al. [1] proposed a secure location proof mechanism, where users and wireless APs exchange their signed public keys to create timestamped location proofs. These schemes are susceptible to collusion attacks where users and wireless APs may collude to create fake proofs. VeriPlace[2] is a location evidence structure which is designed with privacy protection and collusion resilience has been introduced by W.Luo. Hasan et al.[3] proposed a method which relies on both location proofs from wireless APs and witness endorsements from Bluetooth-

UGC Approved Journal
IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2017

enabled mobile peers, so that no users can forge proofs without colluding with both wireless APs and other mobile peers at the same time. It eliminates the necessity of multiple trusted parties. In Davis et al.'s alibi system [5], their private corroborator scheme relies on mobile users within proximity to create alibi's (i.e., evidences) for each other. The safety and privacy of the system is achieved based on a crypto-graphical commitment scheme. Also, multi-level location granularity is not considered in their work.
Cai et al. [7] introduced the model allows a user to explicit his/her privacy needs by way of specifying a public area, which the consumer could sense comfortable if the place is suggested as her vicinity. The recognition of the public vicinity, measured the use of entropy primarily based on its site visitors' footprints interior it, is then used as the person's favored stage of privacy safety. S. Sood et al. [8] introduced password authentication methods in cryptanalysis and their key issues.

III. SYSTEM MODEL AND IMPLEMENTATION

A. Proposed System:
In this paper, an android application called STAMP is presented which enables privacy conserving region evidences for cell users which has goal that provides security and privacy assurance to web consumer's evidences for their previous location visits. This app depends on web application server in vicinity to mutually generate mask id proofs. Trustworthy and non-transferability of location evidences and privateness of users are the main design aims of STAMP. The implementation on Android smart phones indicates that low enumeration and storage sources are required to execute this application.
There are four types of substances in architecture of the system as shown in Fig.1.
A **Prover** is a web server which tries to obtain STP evidences at particular vicinity. A **Witness** is a device which is in proximity with the prover and is willing to prepare an STP evidence for the prover upon receiving his/her request. The witness can be un trusted or may not trusted and the trusted witness can be check-In process.

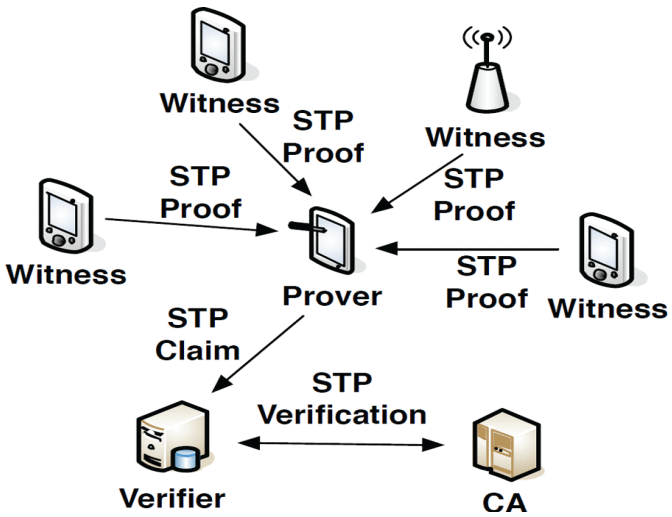

Fig. 1. Architecture of the system

A **Verifier** is the another party that the prover wants to show one or more Spatial-Temporal provenance evidences and claim his/her presence at a location at a particular time. **Certificate Authority (CA)** is a semi-trusted server which issues, manages cryptographic credentials for the other parties. It is also responsible for evidence verification and trust evaluation.

B. Modules Descriptions:
There are four modules involved to run this application.
1. Viewing Hotel List: Client can see the list of hotels and they can registers into hotel by utilizing checks in process.
2.Check In Process: Client will check in to the corresponding hotel, while check in process itself prover will confirm this client is legitimate client or not from social Application database after effective confirmation he will make mask id to the client, this id will be the exceptional id to each clients. Next time that client will be recognized by utilizing the mask id.
3. Feedback in Hotel: Client can give feedback to the hotel, while at the same time prover will check this relating client is now given or not. If given, prover will check the audit date and time. There is some threshold time after this only

UGC Approved Journal
IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2017

client can give their feedback and also it checks for longitude and latitude of place if it matched, then only review will be send successfully otherwise it fails.
4. Process of Spotter Timer: In this module, prover will keep up clock cycle process subsequent to finishing one cycle process. Provers will gather the total number of guests that are visited to hotel and feedbacks will be refreshed to the Social server.
To implement this android application, there are two main algorithms used.
1.Euclidean Distance : We can find the distance between two location using By using this equation that is also called Euclidean Formula.

```
double theta = lon1 - lon2;
double dist = Math.sin(deg2rad(lat1)) * Math.sin(deg2rad(lat2)) + Math.cos(deg2rad(lat1)) * Math.cos(deg2rad(lat2)) * Math.cos(deg2rad(theta));
```

lon1=longitude of location1
lon2= longitude of location2
2.MD5: Message digest algorithm helps to search the hash code of user ID.

IV. RESULTS

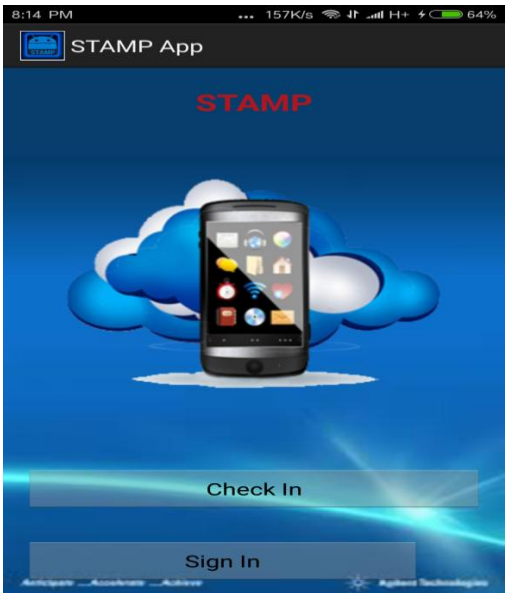

Fig.2. Main page of STAMP application

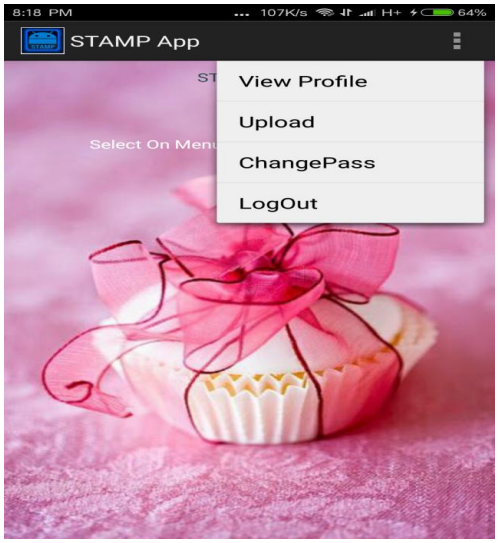

Fig.3. Options in the applications that user can select

UGC Approved Journal
IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2017

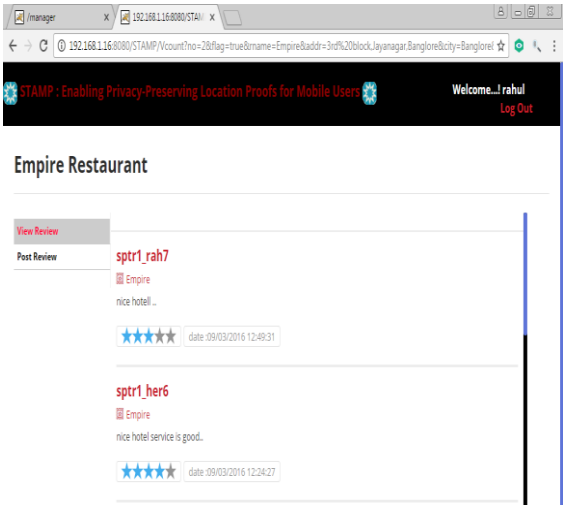

Fig.4. Feedbacks given to hotels by users with their masked id

In this Android application, first user has to register himself/herself by entering details and later he can select check in process to login as shown in fig.2.if user is login, then user can see options first, user profile that includes user personal detailed, second upload option for giving comments for hotels and rating also, third can change password and last he can logout. After uploading the reviews, the original name of user will not show to everybody for the privacy of user and it will display by creating mask id for every user as e depicted in fig. 4.

V. CONCLUSION

In this paper we have implemented an android application called STAMP, which has safety measures and privacy assurance to cell users for their previous location visits. Trustworthiness and non-transferability of location evidences and privacy of users are the main design ambitions of this application with high security assurance. The main advantage of this application is user's privateness because when user give feedback/rating about hotel then nobody can identify the original user name because it displays the user name by generating the masked id for particular user.

ACKNOWLEDGEMENT

I would like to sincerely thank **Prof. Vivekanandreddy,** for his support and encouragement.

REFERENCES

[1] Saroiu and A. Wolman, "Enabling new mobile applications with location proofs", in Proc. ACM HotMobile, 2009
[2] W. Luo and U. Hengartner, "VeriPlace: A privacy-aware location proof architecture", in Proc. ACM GIS, 2010.
[3] R. Hasan and R. Burns, "Where have you been? secure location provenance for mobile devices", CoRR,2011.
[4] I. Krontiris, F. Freiling, and T. Dimitriou, "Location privacy in urban sensing networks: Research challenges and directions," IEEE Wireless,2010.
[5] B. Davis, H. Chen, and M. Franklin, "Privacy preserving alibi systems," in Proc. ACM ASIACCS, 2012.
[6] I. Afyouni, C. Ray, and C. Claramunt, "Spatial models for contextaware indoor navigation systems: A survey," J. Spatial Inf. Sci., no. 4, pp. 85–123, 2014.
[7] T. Xu and Y. Cai, "Feeling-Based Location Privacy Protection for Location-Based Services," Proc.16th ACM Conf. Computer Comm. Security (CCS), 2009.
[8] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.