Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 01, January -2018

STAMP

[1]Karan Mane, [2]Manoj Kamble, [3]Paresh Malpure, [4]Mayur

[1]*BE, Student, DY Patil, Pimpri, Pune, Maharashtra, India*
[2]*BE, Student, DY Patil, Pimpri, Pune, Maharashtra, India*
[3]*BE, Student, DY Patil, Pimpri, Pune, Maharashtra, India*
[4]*BE, Student, DY Patil, Pimpri, Pune, Maharashtra, India*

Abstract *—Location-based services are becoming immensely popular. In addition to services based on users' current geographical location, many potential services rely on users' geographical location history, or their spatial-temporal provenance. Malicious users may lie about their spatial-temporal provenance without a carefully designed security system for users to prove their past locations. In this paper, we present the Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme [1]. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP make sure the binding and non-transferability of the geographical location proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach. Our prototype implementation on the Android platform shows that STAMP is low-cost in terms of computational and storage resources [2]. Extensive simulation experiments show that our entropy-based trust model is able to achieve high collusion detection accuracy.*

Keywords- *Secure Location Authentication, Secure Location Verification, Sensor Networks.*

I. INTRODUCTION

Location-based services are quickly changing into immensely standard. Additionally to services supported users' current location, several potential services deem users' location history, or their spatial-temporal source. Malicious users might slug their spatial-temporal source without a carefully designed security system for users to prove their past locations.

STAMP is designed for ad - hoc mobile users generating location proofs for every alternative in a distributed setting. However, it will simply accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects users' privacy. Our prototype implementation on the android platform shows that STAMP is cheap in terms of computational and storage resources.

Extensive simulation experiments show that our entropy-based trust model is ready to achieve high collusion detection accuracy. The privacy protective location proofs for mobile users can be demonstrated by our application known as location proof. An organization that promotes green commuting and wellness might reward their staff World Health Organization walk or bike to figure. The corporate might encourage daily walking goals of some fixed number of miles. Staff have to be compelled to prove their past commuting paths to the company along with time history. This helps the company in reducing the health care insurance rates and move towards sustainable lifestyle. Location will be shared in secret to others without the interference of third party.

II. LITERATURE SURVEY

According to literature survey after studying different IEEE paper, collected some related papers and documents some of the point discussed here:

1. Title: Enabling New Mobile Applications with Location Proofs (2009)[8]

Author: Stefan Saroiu, Alec Wolman

Description: Location is apace changing into consequent “killer application” as location-enabled mobile hand-held devices proliferate. One category of applications that has yet-to-emerge square measure those during which users have AN incentive to idle their location. These applications cannot believe exclusively on the users’ devices to find ANd transmit location info as a result of users have an incentive to cheat. Instead, such applications need their users to prove their locations. sadly, today’s mobile users lack a mechanism to prove their current or past locations. Consequently, these applications have nonetheless to require off despite their potential. This paper presents location proofs – a straightforward mechanism that permits the emergence of mobile applications that need “proof” of a user’s location. A location proof may be a piece of knowledge that certifies a receiver to a geographical location. Location proofs square measure bimanual out by the wireless infrastructure (e.g., a Wi-Fi access purpose or a cell tower) to mobile devices. The comparatively short vary of the wireless radios ensures that these devices square measure in physical proximity to the wireless transmitter. As a result, these devices square measure capable of proving their current or past locations to mobile applications. during this paper, we tend to begin by describing a mechanism to implement location proofs. we tend to then gift a collection of six future applications that need location proofs to change their core practicality.

2. Title: VeriPlace: A Privacy-Aware Location Proof Architecture (2010)[9]
Authors: Wanying Luo & Urs Hengartner
Description: Recently, there has been a dramatic increase in the number of location-based services, with services like Foursquare or Yelp having hundreds of thousands of users. A user's location is a crucial factor for enabling these services. Many services rely on users to correctly report their location. However, if there is an incentive, users might lie about their location. A location proof architecture enables users to collect proofs for being at a location and services to validate these proofs. It is essential that this proof collection and validation does not violate user privacy. We introduce VeriPlace, a location proof architecture with user privacy as a key design component. In addition, VeriPlace can detect cheating users who collect proofs for places where they are not located. We also present an implementation and a performance evaluation of VeriPlace and its integration with Yelp.

3. Title: Secure Verification of Location Claims (2003)[10]
Authors: Naveen Sastry, Umesh Shankar , David Wagner
Description: With the growing prevalence of sensor and wireless networks comes a new demand for location-based access control mechanisms. We introduce the concept of secure location verifi- cation, and we show how it can be used for location-based access control. Then, we present the Echo protocol, a simple method for secure location verification. The Echo protocol is extremely lightweight: it does not require time synchronization, cryptography, or very precise clocks. Hence, we believe that it is well suited for use in small, cheap, mobile devices

4. Title: Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System (2013)[11]
Author: Zhichao Zhu, Student Member, IEEE, and Guohong Cao, Fellow, IEEE.
Description: Today's location-sensitive service relies on user's mobile device to determine the current location. This allows malicious users to access a restricted resource or provide bogus alibis by cheating on their locations. To address this issue, we propose A Privacy-Preserving LocAtion proof Updating System (APPLAUS) in which collocated Bluetooth enabled mobile devices mutually generate location proofs and send updates 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 and decide whether and when to accept the location proof requests. In order to defend against colluding attacks, we also present between ness ranking-based and correlation clustering-based approaches for outlier detection. APPLAUS can be implemented with existing network infrastructure, and can be easily deployed in Bluetooth enabled mobile devices with little computation or power cost. Extensive experimental results show that APPLAUS can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks.

5. Title: Privacy-Preserving Alibi Systems (2012)[12]
Authors: Benjamin Davis, Hao Chen, Matthew Franklin Description: An alibi provides evidence of a person's past location and can be critical in proving her innocence. An alibi must be bound to a person's identity to prevent from being transferred to another person; however, requiring a person to reveal her identity during alibi creation would compromise the person's privacy. We propose a privacy-preserving alibi system, where a user conceals her identity during alibi creation. The user's identity is revealed only when she chooses to present her alibi to a judge. We design two privacy preserving alibi schemes. In the first scheme, the alibi corroborator is a public entity and therefore needs no privacy protection. Our second scheme protects the privacy of the corroborator as well, where the identity of the corroborator is revealed only when he chooses to help the alibi owner to present her alibi to the judge. We discuss the properties of our schemes and demonstrate their advantages over current alibis. As ubiquitous mobile computing presents an attractive platform for deploying our schemes, we have implemented our schemes on an Android device and shown its satisfactory performance.

III. EXISTING SYSTEM

Existing schemes which require multiple trusted or semi-trusted 3rd parties, STAMP need only Single semi-trusted 3rd party which will embedded in a Certificate Authority (CA). We design our system with an objective of protecting users' anonymity and location privacy. No 3rd parties other than verifiers could see both a user's identity and STP info (verifiers need both identity and STP info in order to perform verification and provide services). Users are given the flexibility to choose the location granularity level that is revealed to the verifier. We examine two types of collusion attacks: (1) A user who is at an intended location masquerades another colluding user and obtains STP proofs for. This attack has never been addressed in any existing STP proof schemes. (2) Colluding users mutually generate fake STP proofs for each other. There have been efforts to address this type of collusion. However, existing solutions suffer from high computational cost and low scalability. Particularly, the latter collusion scenario is in fact the challenging Terrorist Fraud attack, which is a critical issue for our targeted system, but none of the existing systems has addressed it.

IV. PROPOSED SYSTEM

In proposed system we have implement to prove user is review truth to lie on basis of user past location or not user reach destination after reach destination location and share location proof in secure way(attacker should no find user location)so Encrypt location and share data send key to Prover mail. User also view comment and give comment in second module Prover will verify user destination location using key Prover will also check particular comment is truth or lie and display truth comment on android phone to particular user

V. SYSTEM ARCHITECTURE

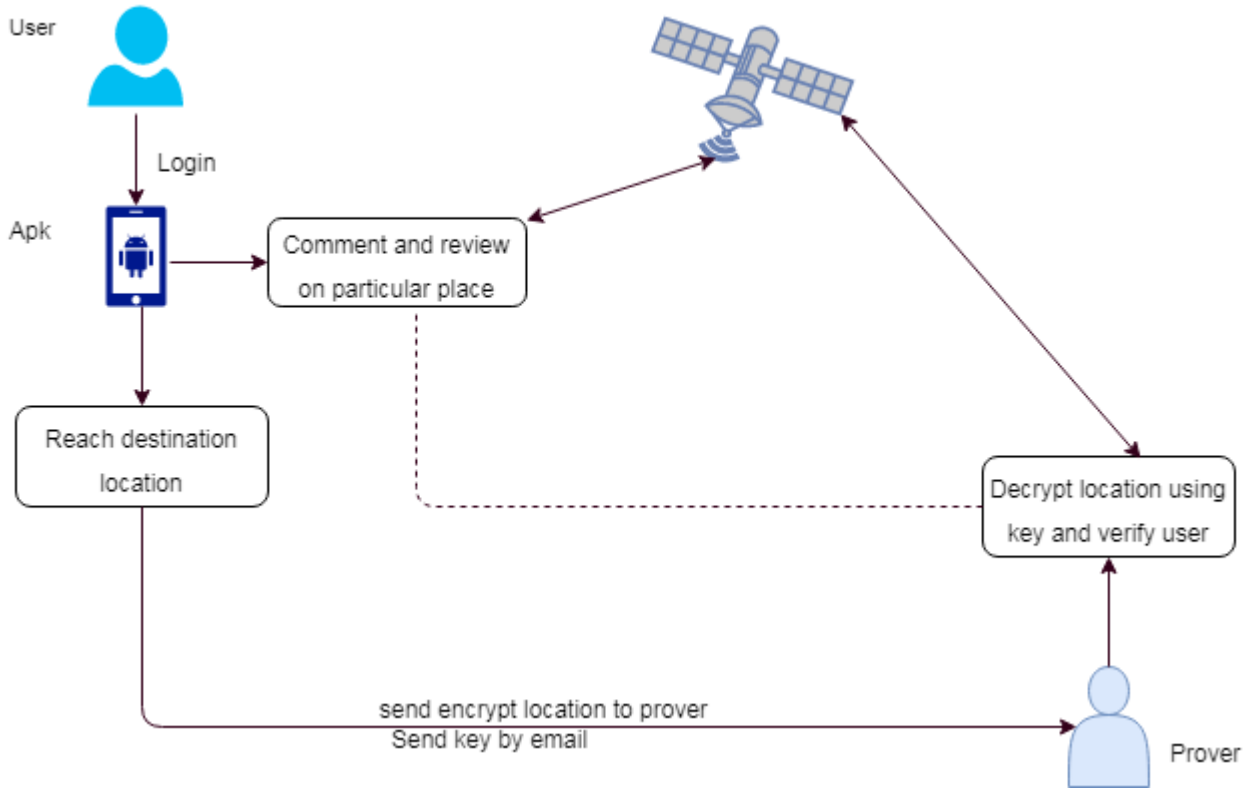

Diagram: System Architecture

VI. CONCLUSION

In this paper we've given STAMP, this aims at providing security and privacy assurance to mobile users' proofs for his or her past location visits. STAMP depends on mobile devices in locality to reciprocally generate location proofs or uses wireless APs to generate location proofs. Integrity and non-transferability of location proofs and location privacy of users are the most design goals of STAMP.

REFRENCES

[1] W. Luo and U. Hengartner, "Proving Your Location Without Giving Up Your Privacy," Proc. ACM 11th Workshop Mobile Computing Systems and Applications (HotMobile '10), 2010.
[2] S. Saroiu and A. Wolman, "Enabling New Mobile Applications with Location Proofs," Proc. ACM 10th Workshop Mobile Computing Systems and Applications (HotMobile '09), 2009.
[3]. V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-Based Trust for Mobile User-Generate Content: Applications Challenges and Implementations," Proc. Ninth Workshop Mobile Computing Systems and Applications 2008
[4] T. Xu and Y. Cai, "Feeling-Based Location Privacy Protection for Location-Based Services," Proc. 16th ACM Conf. Computer Comm. Security (CCS), 2009.
[5]. Zhichao Zhu, Student Member, IEEE, and Guohong Cao, Fellow, IEEE "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System", IEEE TRANSACTIONS ON MOBILE COMPUTING,VOL.12.NO 1 JANUARY 2013
[6] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.C. Herrera, A.M. Bayen, M. Annavaram, and Q. Jacobson,"Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring," Proc. ACM MobiSys, 2008.

[7] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy," Proc. Fifth ACM Workshop Privacy in Electronic Soc., 2006. http://www.parse.com
[8] Stefan Saroiu, Alec Wolman, "Enabling New Mobile Applications with Location Proofs" , Proceedings of the 10th Workshop on Mobile Computing Systems and Applications, HotMobile 2009, Santa Cruz, California, USA, February 23-24, 2009
[9] Wanying Luo & Urs Hengartner, "VeriPlace: A Privacy-Aware Location Proof Architecture", ACM GIS '10, November 2–5, 2010, San Jose, CA, USA, Copyright 2010 ACM 978-1-4503-0428-3/10/11
[10] Naveen Sastry, Umesh Shankar , David Wagner "Secure Verification of Location Claims" , WiSE'03, September 19, 2003, San Diego, California, USA. Copyright 2003 ACM 1581137699/ 03/0009
[11] Zhichao Zhu, Student Member, IEEE, and Guohong Cao, Fellow, IEEE , "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System", IEEE Transactions on Mobile Computing (Volume: 12, Issue: 1, Jan. 2013)
[12] Benjamin Davis, Hao Chen, Matthew Franklin, "Privacy-Preserving Alibi Systems", ACM New York, NY, USA ©2012 ISBN: 978-1-4503-1648-4

