International Journal for Modern Trends in Science and Technology, 8(09): 173-177, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809036
Available online at: http://www.ijmtst.com/vol8issue09.html

A Framework for Proof Generation and Verification in Secure and Private Locations (Pasport)

K Sai Ganesh [1] | P Srinivasa Reddy [2]

[1]Master of Computer Applications (MCA), SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India
[2]Associate Professor in Computer science, SVKP &Dr K S Raju Arts & Science College(A), Penugonda, W.G.Dt., A.P, India

To Cite this Article
K Sai Ganesh and P Srinivasa Reddy A Framework for Proof Generation and Verification in Secure and Private Locations (Pasport). International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 173-177. https://doi.org/10.46501/IJMTST0809036

Article Info
Received: 22 August 2022; Accepted: 12 September 2022; Published: 17 September 2022.

ABSTRACT

Currently, there was a speedy increase in area primarily based structures and applications wherein users submit their region data to provider vendors with a purpose to gain get entry to to a service, resource, or reward. we've visible that in these applications, cheating customers have an incentive to cheat on their place. lamentably, no effective protection mechanism has been adopted by service vendors in opposition to these fake region submissions. this is a vital issue that reasons severe outcomes for those programs. prompted through this, we recommend the privateness-aware and cozy evidence Of pRoximiTy (PASPORT) scheme in this article to deal with the problem. the use of PASPORT, customers post a area evidence (LP) to service vendors to prove that their submitted location is real. PASPORT has a decentralized architecture designed for advert hoc scenarios in which mobile customers can act as witnesses and generate LPs for every different. It gives consumer privateness safety in addition to protection homes, including unforgeability and non transferability of LPs. moreover, the PASPORT scheme is resilient to prover–prover collusions and considerably reduces the fulfillment opportunity of Prover–Witness collusion attacks. To further make the proximity checking system private, we suggest P-TREAD, a privacy-aware distance bounding protocol and combine it into PASPORT. To validate our version, we put in force a prototype of the proposed scheme on the Android platform. good sized experiments suggest that the proposed approach can successfully shield area-based totally packages towards fake submissions

KEYWORDS:Distance bounding (DB), location privacy, location proof (LP) location-based services

1. INTRODUCTION

Recent advances in smartphone technology and location systems have given rise to a wide variety of location-based applications and services [1]-[3],[48]. Radio Networks (CRN) and location-based access control systems. In these applications, mobile her users transmit their location information to location-based service her providers (LBSPs) to obtain access to services, resources, or rewards. These applications are very popular due to the convenient services they provide. According to a recent business report, the market value of LBS was $20.53 billion in 2017 and is expected to reach $133 billion in 2023, with a projected CAGR of 36.55%[4].].

However, LBSP is vulnerable to location spoofing attacks because unauthorized users are tricked into lying about their location and sending bogus location data [5]–[9]. Here are some examples to highlight issues related to

these applications. Current online ratings and review applications do not verify a user's physical location, allowing users to post fake positive or negative reviews of their company or competitors [10], [11]. .
Additionally, malicious users of CRNs [6], [8], [16] can submit fake locations to the database to access channels that are not available at that location. Location-based access control applications [18]–[20] allow an attacker to gain unauthorized access to a system or resource by submitting spoofed location claims. In activity tracking applications, insurers can offer health insurance plans that offer discounts if customers demonstrate a minimum level of physical activity [7], [12]–[15]. This creates an incentive for rogue users to spoof their location data. So far, based on these examples, it's clear that preventing these applications from sending fake location information is still an open question. Many location proof (LP) schemes have been proposed to protect these applications from location spoofing attacks. Using these mechanisms, a mobile device (called a prover in the literature) receives one or more LPs from neighboring devices when he visits a site.

The verifier then sends the received LP as a location claim to her LBSP. LBSP will review the submitted LP and either approve or deny the user's claim. LP schemes are divided into two groups, centralized or decentralized, depending on the system architecture. In a centralized mechanism [21]-[24], trusted wireless infrastructure [e.g. WiFi access points (APs)] are used to generate LPs for mobile users. In decentralized schemes [25]–[30], mobile users act as witnesses and generate LPs with each other. The latter is suitable when there is no wireless infrastructure in the desired location or when deploying a large number of APs in various locations is expensive. Our extensive literature review and to the best of our knowledge show that all current LP schemes have at least one major drawback.

First, a number of those schemes are inclined to prover–prover (P–P)collusions [22], [25], [2]. In this attack, a far flung malicious prover colludes with a cheating consumer (positioned at a preferred site) to gain an LP. The cheating consumer submits an LP request to the neighbor witness gadgets on behalf of the far flung prover. This protection danger is known as terrorist fraud withinside the literature [31], [32] (see Section III-A for extra details). Second, not one of the cutting-edge disbursed schemes provide a dependable answer for Prover–Witness (P–W) collusions. In this attack, a bent consumer acts as a witness for a far flung malicious prover and generates a faux LP for him [25]. Note that this protection danger is unique to the disbursed LP schemes handiest in view that witnesses aren't relied on in this sort of scheme. Finally, in a few schemes, area privateness has now no longer been considered [21], [23], [28], i.e., customers broadcast their identification for neighbor gadgets or a 3rd birthday birthday celebration server all through the LP technology or submission process. In addition, there are different demanding situations with the cutting-edge schemes, which includes high degree of verbal exchange and computation overheads [26] and expensive implementation [21], [24].

As a long way as we know, no LP scheme has been added to cope with all those demanding situations on the identical time. Motivated with the aid of using this, to cope with those key concerns, we propos a disbursed LP scheme, Privacy-Aware and Secure Proof Of proximity (PASPORT), which plays LP technology and verification for cellular customers in a steady and privateness-conscious manner. The proposed scheme affords the integrity and non transferability of generated LPs. To make PASPORT immune to P–P collusions and carry out private proximity checking, we increase a privateness conscious distance bounding (DB) protocol P-TREAD and combine it into PASPORT. P-TREAD is a changed model of TREAD [33], a nation of the artwork and steady DB protocol with out privateness consideration. Our customization does now no longer have an effect on TREAD's foremost shape and features.

Thus, PASPORT advantages from its protection guarantees. By employing P-TREAD because the DB mechanism, a malicious prover colluding with an adversary can effortlessly be impersonated with the aid of using the adversary later. Generally, customers do now no longer take any such danger with the aid of using starting up a

prover–prover collusion. The contributions of this article are threefold.1) We layout PASPORT, a steady, privateness-conscious and collusion-resistant LP scheme for cellular customers. PASPORT has a decentralized structure appropriate for eventualities wh erein a set wi-fi infrastructure does now no longer exist. 2) To privately carry out the technique of proximity checking, we advocate P-TREAD, a privateness-conscious and secured mechanism and combine it into PASPORT. 3) We carry out a prototype implementation of PASPORT at the Android platform. Our experimental outcomes display that the proposed scheme works faster than the present disbursed LP schemes and calls for low computational resources.

In the relaxation of this article, the associated paintings is mentioned in Section II. We gift the preliminaries in Section III. In Section IV, we introduce the PASPORT scheme. A theoretical evaluation is furnished in Section V. We speak the experimental outcomes in Section VI, and a few in addition discussions are in Section VII. Finally, we finish this newsletter in Section VIII with the aid of using providing a summaryandfuture paintings

2. LITERATURE SURVEY

The recent advances in smartphone technology and positioning systems has enabled social network service providers to offer a variety of location–based applications and services for their users. In these applications, real–time location data of mobile users is utilised to provide requested information or access to a resource or service. The variety of useful services offered by these applications has made them very popular [14], [17–19]. However, preserving location privacy of users is a big challenge for the service providers since users share their location data either with other users or with a service provider.

This chapter presents a literature review on the current privacy preserving techniques and solutions in social networks. This includes the privacy preserving mechanisms proposed based on the popular differential privacy framework. We also discuss the current location privacy preservation mechanisms proposed for Location–Base Services (LBS) and Geo–Social Networks (GeoSNs). In this regard, K–Anonymity, Dummy–Based, and Cryptography–Based schemes are reviewed.

Privacy protection in social networks has been comprehensively studied by Abawajy et al. [59] to present a comprehensive survey of the recent developments in social networks' data publishing. They have analysed different privacy risks and attacks in social media along with the presentation of a threat model. They have also quantified and classified the background knowledge which is used by adversaries to violate users' privacy. In addition, Fire et al. [60] presented some strategies and methods in privacy preserving social network data publishing through a detailed review of different security and privacy issues. They have reviewed a range of existing solutions for these privacy issues along with eight simple–to–implement recommendations which can improve users' security and privacy when using these platforms [13].

A few location privacy protection mechanisms have been proposed based on differential privacy. In [64], a perturbation technique based on differential privacy was introduced to achieve geo–indistinguishability for protecting the exact location of a user. This technique adds random Laplace–distributed noise to users' location in order to sanitize their location before publishing. A differentially private hierarchical location sanitization (DPHLS) approach has been proposed for location privacy protection in large–scale user trajectories. The approach provides a personalised hierarchical mechanism that protects a user's location privacy by hiding the location in a dataset that includes a subset of all possible locations that might be visited in a region [65]. By doing this, the level of location randomisation is reduced, hence, the amount of noise required for satisfying differential privacy conditions is minimized.

Some other research studies have recently been done on the location privacy of Geo–Social Networks (GeoSNs) users [61], [67–69]. GeoSNs are a variety of social networks by which users can find their favourite events, persons or groups in a specific region or identify popular places by comparing how many people have already checked–in at different places. This is done by utilising users' location data which have been shared by them in that region. In fact, GeoSNs combine location recommendation services (such as services offered by location–based services) with social network

functionality [10], [69]. In other words, they can be viewed as location–based social networks which connect people in a specific region based on their interests.

In [69] different GeoSNs were classified into three categories Content–Centric, Check–In Based and Tracking–Based according to the services they offer. In addition, the main privacy issues that threaten user location privacy were identified. Moreover, the authors of [67] have studied techniques that sanitize users' location data based on differential privacy framework before publishing them as location recommendations in GeoSNs. Moreover, to enhance the accuracy of the location recommendations, they have identified some effective factors which improve data accuracy.

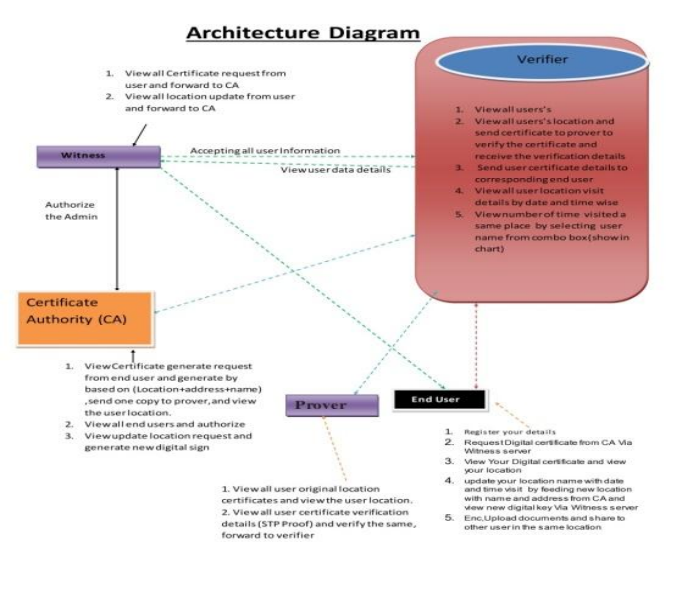
3. PROBLEM STATEMENT

To address this issue, Saroiu and Wolman proposed a technique in which the AP broadcasts beacon frames consisted of a sequence number. To obtain an LP, users must sign the last transmitted sequence number with their private key and send it back to the AP along with their public key (the access point broadcasts beacons every 100 ms). This makes the system resistant against terrorist frauds since the malicious prover does not have enough time to receive the sequence number from the adversary and sign and send it back to the adversary. However, the proposed algorithm has privacy issues because users must reveal their identity publicly. In addition, the user`s identity is revealed publicly, which might cause privacy issues.proposed a privacy-preserving alibi (LP) scheme that has a distributed architecture. To preserve users` location privacy, in the introduced scheme, their identity is not revealed, while an alibi is being created. Prover-Witness collusions have not been discussed although it provides an efficient and privacy-aware platform for users to create LPs for other users is another example in which an entropy-based trust model is proposed to address the Prover-Witness collusions issue. This method is also unable to provide the necessary reliability to detect Prover- Witness collusions. Moreover, the computation time required by STAMP to create an LP is long when users have a large private key. Although different novel methods have been introduced so far, each of them has its own constraints, i.e., privacy issues vulnerability against collusions high level of communication and computation overheads and expensive for implementation. The scheme proposed in prevents P–W collusions only in crowded scenarios.

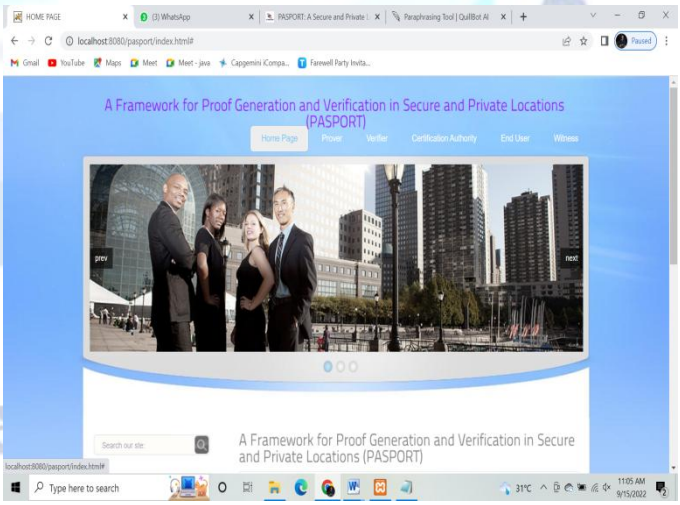
4. METHODOLOGY

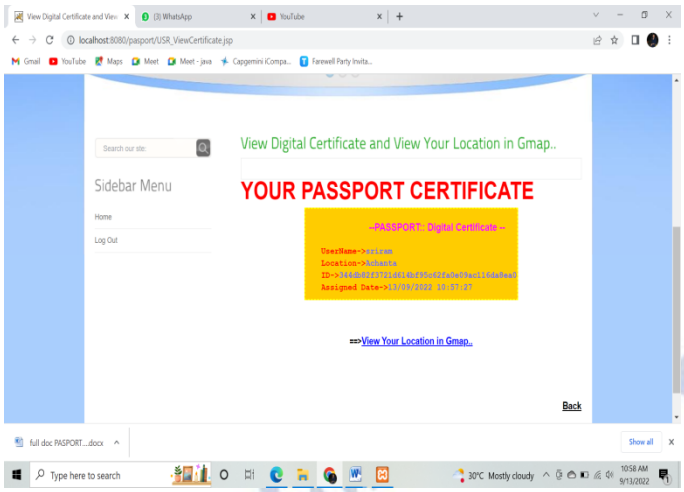
In this section, we present our proposed scheme for secure LP generation and verification. First, we present the framework and its entities. Second, we present the trust and threat model which we have considered in this article. Following this, we introduce P-TREAD. Finally, the full framework of the PASPORT scheme is presented.

5. ARCHITECHTURE:



6. RESULTS





7.CONCLUSION

This article proposed a secure and privacy-aware scheme for LP generation and verification. The proposed scheme has a decentralized architecture suitable for ad hoc applications in which mobile users generate LPs for each other. Furthermore, we employed a witness selection mechanism to address the prover–witness collusions. Using the proposed mechanism, available witnesses are randomly assigned to requesting provers by the verifier. As a future work direction, we intend to extend the PASPORT scheme such that it provides location granularity feature. Moreover, designing a blockchainbased incentive mechanism to encourage users to collaborate with thesystem can be another research direction for this article.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] P. Asuquo et al., "Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges, and countermeasures," IEEE Internet Things J., vol. 5, no. 6, pp. 4778–4802, Dec. 2018.

[2] Q. D. Vo and P. De, "A survey of fingerprint-based outdoor localization," IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 491–506, 1st Quart., 2016.

[3] R. Gupta and U. P. Rao, "An exploration to location–based service and its privacy preserving techniques: A survey," Wireless Pers. Commun., vol. 96, no. 2, pp. 1973–2007, 2017.

[4] Global Location–Based Services Market (2018–2023). Accessed: Jul. 20, 2019.[Online]. Available: https://www.businesswire.com/news/home/20180927005490/en/Global–Location-based-Services-Market2018-2023-Projected-Grow

[5] Y. Zheng, M. Li, W. Lou, and Y. T. Hou, "Location based handshake and private proximity test with location tags," IEEE Trans. Depend. Sec. Comput., vol. 14, no. 4, pp. 406–419, Jul./Aug. 2017.

[6] Y. Li, L. Zhou, H. Zhu, and L. Sun, "Privacy–preserving location proof for securing large–scale database–driven cognitive radio networks," IEEE Internet Things J., vol. 3, no. 4, pp. 563–571, Aug. 2016.

[7] A. Pham, K. Huguenin, I. Bilogrevic, I. Dacosta, and J. P. Hubaux, "SecureRun: Cheat–proof and private summaries for location–based activities," IEEE Trans. Mobile Comput., vol. 15, no. 8, pp. 2109–2123, Aug. 2016.

[8] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in Proc. IEEE INFOCOM, Apr. 2013, pp. 2751–2759.

[9] Z. Zhang et al., "On the validity of geosocial mobility traces," in Proc. ACM Workshop Hot Topics Netw.(HotNets), 2013.

[10] D. Bucher, D. Rudi, and R. Buffat, "Captcha your location proof—A novel method for passive location proofs in adversarial environments," in Proc. 14th Int. Conf. Location Based Services, 2018, pp. 269–291.

[11] A. Mukherjee, B. Liu, and N. Glance, "Spotting fake reviewer groups in consumer reviews," in Proc. 21st Int. Conf. World Wide Web (WWW), 2012, pp. 191–200.

[12] Nike+ Badges and Trophies. Accessed: Jul. 20, 2019.[Online]. Available: http://www.garcard.com/nikeplus.php

[13] Higi. Higi: Know Your Numbers. Own Your Health. Accessed: Jul. 20, 2019.[Online]. Available: https://higi.com

[14] Oscar Health Using Misfit Wearables To Reward Fit Customers. Accessed: Jul. 20, 2019.[Online]. Available: http://www.forbes.com/sites/stevenbertoni/2014/12/08/oscarhealth-using-misfit-wearables-toreward-fit-customers

[15] Health Insurer's App Helps Users Track Themselves. Accessed: Jul. 20, 2019.[Online]. Available: http://www.technologyreview.com/news/516176/healthinsurers-app-helps-users-track-themselves

Authors Biography

K.Sai Ganesh currently pursuing MCA in SVKP & Dr.K.S Raju Arts & Science College affiliated to Adikavi Nannaya University, Rajamahendravaram. His research interests include Data Structures, Web Technologies, Operating Systems, Data Science and

P.Srinivasa Reddy is working as Associate Professor in SVKP &Dr K S Raju Arts & Science College, Penugonda, A.P. He received Masters Degree in Computer Applications from Andhra University. His research interests include Operational, Research ,Probability and Statistics , Design and Analysis of algorithm , Big Data Analytics