iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50394

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

PASPORT: A Secure and Private Location Proof Generation and Verification Framework

Prof. Vaishali Surjuse[1], Dhushant Isankar[2], Mrunali Kamble[3]
[1]*Department of Computer Technology, KDKCE, Nagpur, India*
[2, 3]*Projectee, Department of CT, KDKCE, Nagpur, India*

Abstract: ***Recently, there has been a rapid growth in locationbased systems and applications in which users submit their location information to service providers in order to gain access to a service, resource, or reward. We have seen that in these applications, dishonest users have an incentive to cheat on their location. Unfortunately, no effective protection mechanism has been adopted by service providers against these fake location submissions. This is a critical issue that causes severe consequences for these applications. Motivated by this, we propose the Privacy-Aware and Secure Proof Of pRoximiTy (PASPORT) scheme in this article to address the problem. Using PASPORT, users submit a location proof (LP) to service providers to prove that their submitted location is true. PASPORT has a decentralized architecture designed for ad hoc scenarios in which mobile users can act as witnesses and generate LPs for each other. It provides user privacy protection as well as security properties, such as unforgeability and non transferability of LPs. Furthermore, the PASPORT scheme is resilient to prover–prover collusions and significantly reduces the success probability of Prover–Witness collusion attacks. To further make the proximity checking process private, we propose P-TREAD, a privacy-aware distance bounding protocol and integrate it into PASPORT. To validate our model, we implement a prototype of the proposed scheme on the Android platform. Extensive experiments indicate that the proposed method can efficiently protect location-based applications against fake submissions***
Keywords: Distance bounding (DB), location privacy, location proof (LP) location-based services (LBSs).

I. INTRODUCTION

The recent advances in the smartphone technology and positioning systems has resulted in the emergence of a variety of location-based applications and services such as activity tracking applications, location-based services (LBSs), database-driven cognitive radio networks (CRNs), and location-based access control systems. In these applications, mobile users submit their position data to a location-based service provider (LBSP) to gain access to a service, resource, or reward. These applications are very popular due to the useful services they offer. According to recent business reports, the market value of LBSs was U.S. $20.53 billion in 2017 and is anticipated to reach U.S. $133 billion in 2023, with an expected annual growth rate of 36.55%. However, LBSPs are vulnerable to location spoofing attacks since dishonest users are incentivized to lie about their location and submit fake position data. This is a critical issue that causes severe consequences for these applications. Motivated by this, we propose the Privacy Aware and Secure Proof Of proximity (PASPORT) to address the problem.

II. AIMS AND OBJECTIVE

This website is used create a decentralized architecture designed for ad hoc scenarios in which mobile users can act as witnesses and generate LPs for each other. it provides user privacy protection as well as security properties, such as un forgetability and non transferability of LPs. Furthermore, the PASPORT scheme is resilient to prover–prover collusions and significantly reduces the success probability of Prover–Witness collusion attacks. To reduce the LOAD of Location based services servers by validating only true locations.To reduce the risk of Unwanted location leaks which may sometimes result in STALKING , KIDNAPPING etc.

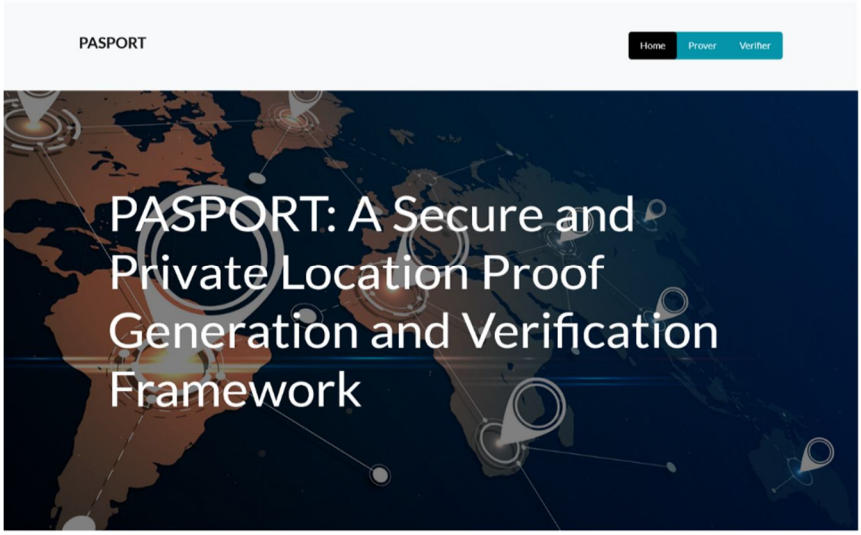
III. PROBLEM STATEMENT

We have seen that in L.B.S applications, dishonest users have an incentive to cheat on their location. Unfortunately, no effective protection mechanism has been adopted by service providers against these fake location submissions. This is a critical issue that causes severe consequences for these applications. LBSPs are vulnerable to location spoofing attacks since dishonest users are incentivized to lie about their location and submit fake position data .In the current online rating and review applications, users' real location is not verified, which enables them to submit fake positive or negative reviews for their own business or their rivals.

Furthermore, in CRNs , malicious users can submit fake locations to the database to access channels that are not available in their location. In location-based access control applications, attackers can gain unauthorized access to a system or resource by submitting fake location claims.In activity-tracking applications, insurance companies may offer health insurance plans in which customers are offered discounts if they have a minimum level of physical activity. This creates an incentive for dishonest users to cheat on their location data.

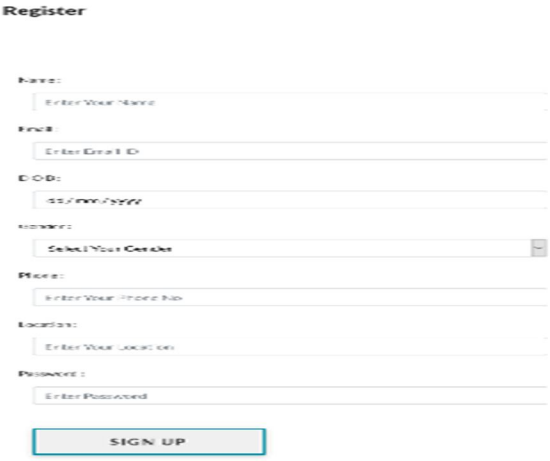
IV. MODULE DESCRIPTION

1) *Architecture and Entities:* The proposed system architecture is the system has a distributed architecture and consists of three types of entities, i.e., prover, witness, and verifier. A prover is a mobile user who requires to prove his/her location to a verifier. A witness is the entity that accepts to issue an LP for a neighboring prover upon request. We assume that service providers create sufficient incentives for mobile users to become a witness and certify other users' location. In PASPORT, we consider witnesses as mobile users. Finally, a verifier is the unit that is authorized by the service provider to verify LPs claimed by provers. We assume that provers communicate with witnesses through a short-range communication interface, such as Wi-Fi or Bluetooth. This short range communication channel is supposed to be anonymous such that users can broadcast their messages over it without revealing their revealing their identifying data, such as IP or MAC address.
2) *Trust and Thread Model:* We assume that mobile users are registered with the service provider. Each user has a unique public-private pair key stored on his/her mobile device and certified by a CA. Users' identity is determined through their public key, and we assume that users never share their private key with other users because they do not give their mobile devices to others Thus, in a collusion scenario, we suppose a malicious prover never goes that far to provide another party with his/her private key. We also assume that all the messages exchanged between the entities might be eavesdropped by passive eavesdroppers. In the following, we discuss the trust and threat model for each entity individually
3) *Prover:* It is assumed that the prover makes an effort to obtain false LPs. This can be done through different scenarios in which a prover might try to provide the witnesses with fake information about his/her location to convince them to generate LPs for him/her, manipulate the LP issued for him/her to change its location or time field, attempt to steal an LP issued for another user and use it for him/herself, and collude with other users (provers or witnesses) to obtain LPs. Moreover, we assume that provers try to obtain the identity of witnesses.
4) *Witness:* A witness might collude with a prover to generate a fake LP for him/her. In addition, a witness may try to deny an LP that has been issued by himself/herself. Witnesses are assumed to be curious about the provers' identity.
5) *Verifier:* We suppose that the verifier is trusted and never leaks users' identity and their spatiotemporal data. It is assumed that the verifier keeps a regularly updated list of witnesses who are present at the given location and have accepted to generate LPs for other users. The verifier accepts the LPs issued by these witnesses only. We suppose that service providers create necessary incentives to encourage selfish users to collaborate with the system. Otherwise, they might not generate LPs to save their battery power or reduce their communication costs.
6) *Login Window:* Here the user can select if they want to be PROVER or VEIFIY someone's location.



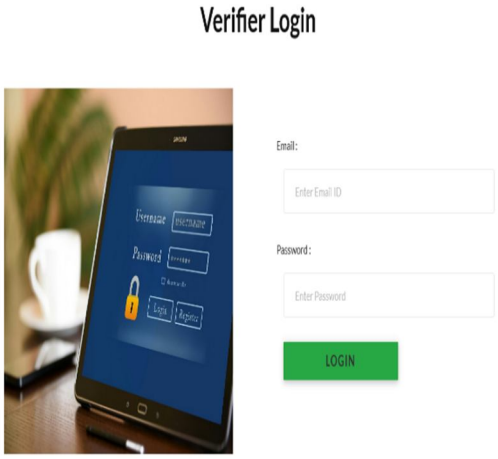
A. Registration Window

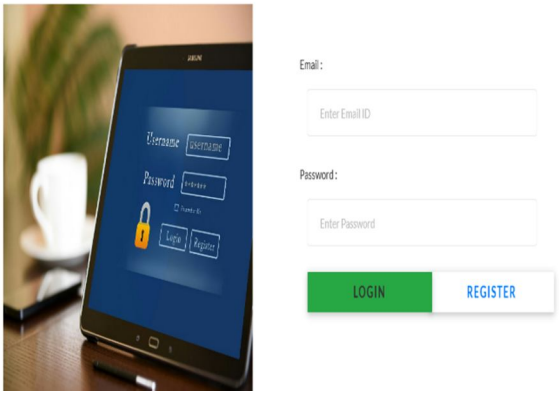
In the REGISTRATION form the user has to fill details like USERNAME, PASSWORD, EMAIL, et



B. USER and VERIFIER Login Page

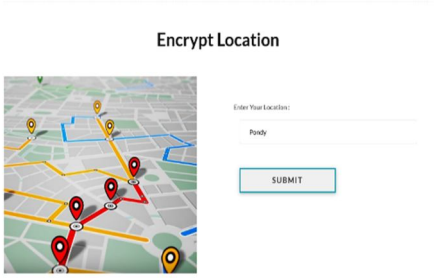
Both the USER and VERIFIER login page has similar U.I but differnet E-mail are required for registration.





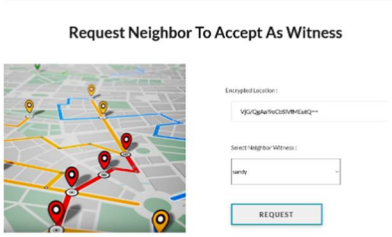
C. Location Encryption Page

User is able to encrypt their location



D. Accept as Witness

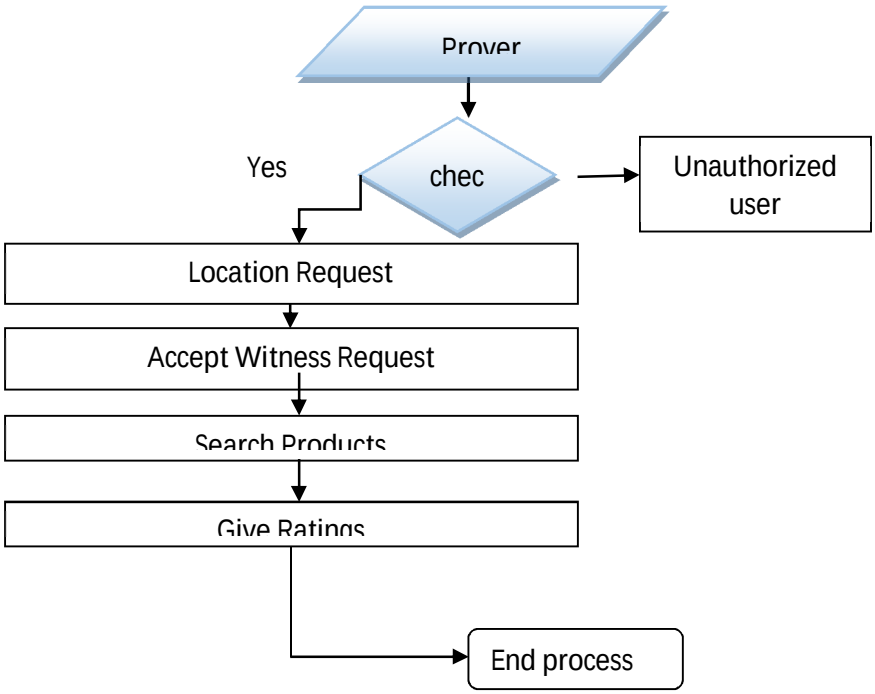
Here the user is able to accept prover's request



V. PROPOSED WORK

We propose a privacy preserving verifiable proximity test for L.B.S (Location based services) which enables the user to verify the correctness of proximity test results from L.B.S servers without revealing their Location information. The Privacy-Aware and Secure Proof Of proximiTy (PASPORT) scheme in this article to address the problem.Using PASPORT, users submit a location proof (LP) to service providers to prove that their submitted location is true.PASPORT has a decentralized architecture designed for ad hoc scenarios in which mobile users can act as witnesses and generate LPs for each other.Furthermore, PASPORT is resilient to prover– prover collusions and significantly reduces the success probability of Prover– Witness collusion attacks.

VI. DFD OF PROPOSED SYSTEM



VII. FUTURE SCOPE

As a future work direction, we intend to extend the PASPORT scheme such that it provides location granularity feature. Using these users can select to which level their location data is revealed. Moreover, designing a block chain based incentive mechanism to encourage users to collaborate with the system can be another research direction for this article.

VIII. RESULT

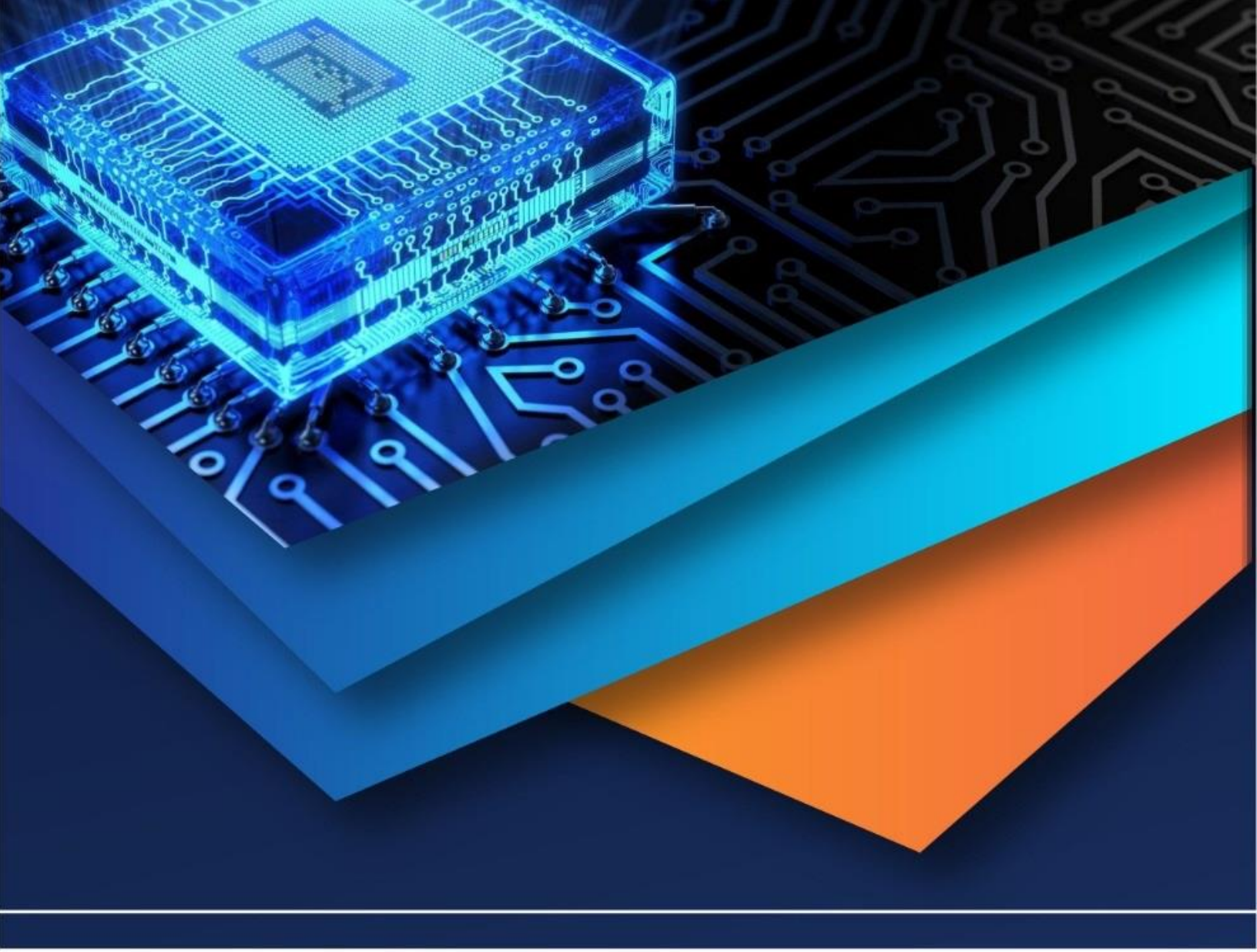
The proposed scheme has a decentralized architecture suitable for ad hoc applications in which mobile users generate LPs for each other.

IX. 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. To address terrorist frauds, we developed a DB protocol PTREAD, that is, a private version of TREAD, and integrated it into PASPORT. Using P-TREAD, a dishonest prover who established a prover-prover collusion with an adversary can easily be impersonated by the adversary later. Thus, no logical user takes such a risk by initiating a prover– prover collusion. 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. This prevents malicious provers from choosing the witnesses themselves.

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–Locationbased-Services-Market- 2018-2023-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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY