International Journal of Modern Developments in Engineering and Science
Volume 1, Issue 6, June 2022
https://www.ijmdes.com | ISSN (Online): 2583-3138

Witness Proof Generation with Security and Verification for Passport Approval

D. Swathi[1*], M. K. Sornalatha[2], S. Yamini[3], S. J. Vivekanandan[4]
[1,2,3]*Student, Department of Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, India*
[4]*Assistant Professor, Department of Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, India*

***Abstract*: Users give their location information to service providers in order to obtain access to a service, resource, or incentive, and location-based systems and applications have exploded in popularity recently. We've seen that dishonest users have an incentive to lie about their whereabouts in these apps. Unfortunately, service providers have not implemented any effective protection methods against these faked location entries. This is a crucial issue with serious implications for these applications. Motivated by this, we present in this paper the Privacy-Aware and Secure Proof Of pRoximiTy (PASPORT) scheme as a solution to the problem. Users submit a location proof (LP) to service providers using PASPORT to prove that the location they provided is valid. PASPORT includes a decentralized architecture that allows mobile users to act as witness and create LPs for one another in ad hoc scenarios. It protects user privacy while also providing security features such as LP unforgeability and non-transferability. Furthermore, the PASPORT method is strong to prover-prover collusions and lowers the risk of Prover-Witness collusion attacks. We propose P-TREAD, a privacy-aware distance bounding mechanism, and incorporate it into PASPORT to make the proximity verification process even more private. We implement a prototype of the proposed method using the Android platform to validate our approach. Extensive testing has shown that the suggested solution effectively protects location-based systems from bogus submissions.**

***Keywords*: Privacy-Aware and Secure Proof Of pRoximiTy (PASPORT), Location proof (LP).**

1. Introduction

Because of the useful services they provide, these programmes are quite popular. LBSs have a market worth of $20.53 billion, according to latest business statistics. Because dishonest users are encouraged to lie about their location and submit bogus position data, LBSPs are vulnerable to location spoofing attacks. Malicious users can submit fake credentials to the database in order to gain access to channels that aren't available in their area. By providing bogus location claims to a location-based access control service, attackers can get unauthorized access to a system or resource. We introduce Privacy-Aware and Secure Proof Of pRoximiTy (PASPORT), a distributed LP system for activity- tracking applications that conducts LP generation and verification for mobile users in a secure and privacy-aware manner. The proposed scheme is open to relay threats, as well as terrorist crimes in particular. In other words, their approach is missing a mechanism that allows the location manager to verify that the received ID matches to the user who submitted the LP request. The suggested technique ensures that created LPs are both secure and non- transferable. Because users must reveal their identities publicly, the suggested algorithm raises privacy concerns. The similar concept was utilized by Javali et al to make their algorithm resistant to relay attacks. The proposed approach has three components: an AP, a verifier, and a server, all of which add to the system's expense. Furthermore, the user's information is publicly disclosed, which may raise privacy risks.

2. System Analysis

A. *Existing System*

According to our exhaustive literature research and to the best of our knowledge, all existing LP methods have at least one major flaw. First, prover– prover (P–P) collusions are a risk for some of these systems. A remote malicious prover collaborates with a fake user to get an LP in this attack. On account of the faraway prover, the dishonest user sends an LP request to the nearby witness devices.

Terrorist fraud is the term used in the literature to represent this security hazard. Further, none of the existing distributed systems can detect Prover– Witness (P–W) collusions. A corrupt user acts as a witness for a virtual rogue prover and generates a bogus LP for him in this attack. This security risk is unique to distributed LP schemes since witnesses cannot be trusted in this sort of scheme. Finally, location privacy has not been acknowledged in certain methods.

Disadvantages:

- The issue with PASPORT is that individuals must provide a location proof (LP) to way that reveals to confirm that the location they provided is correct.
- In a distance hijacking attack, a far hostile prover utilizes the existence of one or more trustworthy provers to offer false information about his location to a truthful verifier.

B. *Proposed System*

The suggested technique ensures that created LPs are both secure and non-transferable. We design and integrate P-

*Corresponding author: dswathi.2112@gmail.com

TREAD, a privacy-aware distance bounding (DB) protocol, into PASPORT to make it resistant to P–P collusions and to do private proximity checks. P-TREAD is a revised form of TREAD, a region and secure database protocol that does not take into account privacy. TREAD's fundamental structure and functionalities are unaffected by our modification. As a result, PASPORT reaps the benefits of its security guarantees. A rogue prover collaborating with an attacker can simply be scammed by the attacker later by using P-TREAD as the Distance Bounding mechanism. By commencing a prover– prover collusion, most users do not accept such a risk. The suggested approach consists of three components: an AP, a verifier, and a server, all of which add to the system's expense. Furthermore, the user's profile is publicly disclosed, which may raise privacy concerns. We are producing all user details using an encryption technique. We are using Identity-Based Broadcast Encryption methods for the encryption methods. During the data transfer data process, the user.

Advantages:

- The proposed technique is quicker than existing distributed LP systems and uses fewer computational power.
- It has privacy concerns because users must disclose their identities openly. The similar concept was utilized by Javelin et al. to make their algorithm immune to relay threats.
- Broadcast encryption techniques allow senders to rapidly distribute cipher-texts to a wide number of receivers while ensuring that only verified receivers are able to decipher them. Public key encryption techniques that use random sequences as public keys are known as identity-based encryption schemes.

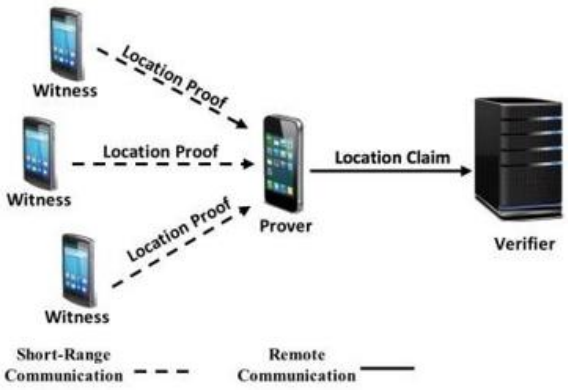

Fig. 1. System architecture

3. Modules Description

A. Prover

We reduce a witness' duty to merely gathering (not validating) the required information so that the provers can submit a Detail report privately to nearby witnesses. information from the prover (here is where the verification is done) via a remote trustworthy verifier) The prover encrypts and sends all security data to a witness who confirms them and returns them to you when the request is submitted to the verifier by the prover. To alert the verifier that he/she wishes to Accept, the prover delivers the following message Report. We use P-TREAD into the method to do provers' proximity verification, which is a simpler protocol despite its security gains over the Bussard-Bagga protocol. We perform our trials for various distances and compare the findings to the performance to determine the impact of geographic constraints between android platforms on LP production.

B. Verifier

The verifier retrieves all witnesses who have just (in a reasonable length of time) shown that they are within an enough of location Loc from its witness database (this acceptable distance is defined depending on the application) after getting the prover's statement. The proposed trust model is then used to select K witnesses from among the nominated witnesses. This prover's K witnesses are then competent to generate LPs. If there are insufficient qualified witnesses, the verifier will put the request on hold until the required shortage of eligible witnesses becomes ready. The verifier then makes a special ID for this LP (LP ID) and transmits it to the chosen witnesses as well as the prover.

C. Prover Location Privacy

In messages Request, m1, and m4, the prover's ID displays. The public key of the verifier secures these messages. As a result, only the verifier has the ability to recognize the prover, and neither the witnesses nor an observer can see the prover's identification. The sign-then-encrypt technique, as previously mentioned, increases PASPORT's capacity to protect users' location privacy.

D. Witness Location Privacy

Due to the fact that a witness device encrypts its ID utilizing, it is not possible for the prover to access the verifier's public key. Alternatively, an eavesdropper could be used to track down the witness. Also, users' autographs do not expose their names, they are private of the sign-then-encrypt model that was used.

E. Witness Trust Model

The PASPORT witness ranking system now includes an entropy-based trust concept. The verifier calculates a threshold for a witness device based on its LP creation history using this trust model. The device is chosen to witness for a seeking prover if the resulting score exceeds a criterion. In fact, if a witness device meets the criterion, it is chosen to be a witness for a seeking prover. In fact, if a witness device has issued a large number of LPs for that prover, it will obtain a poor score. As a result, the prover mechanism is unable to receive LPs from a select group of witnesses. Entropy is the overall amount of information obtained from a message generated by a random source of data in information theory. It is based on the notion that when a minimal message is received, it contains more data than when a slightly elevated message is generated by the source of data. As a result, it is an appropriate measure of the level of flexibility and unpredictability that a prover device's witness list should include.

4. Results

Fig. 2. Home page

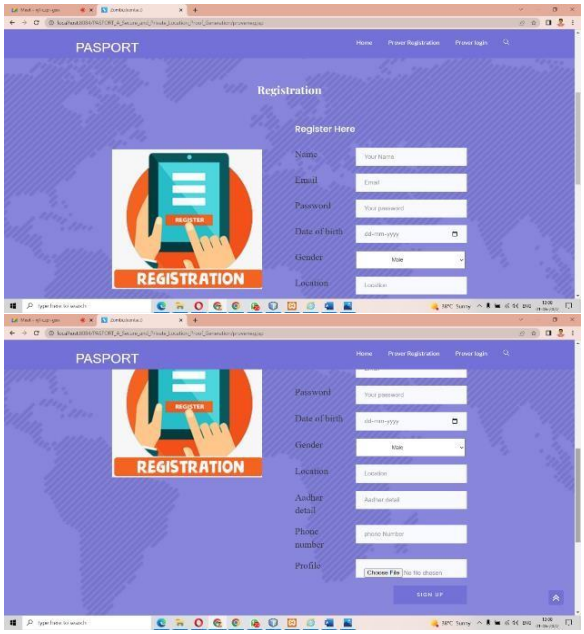

Fig. 3. Prover registration

Fig. 4. Prover login

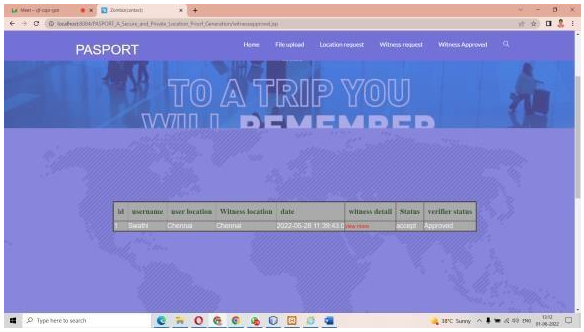

Fig. 5. Witness approval

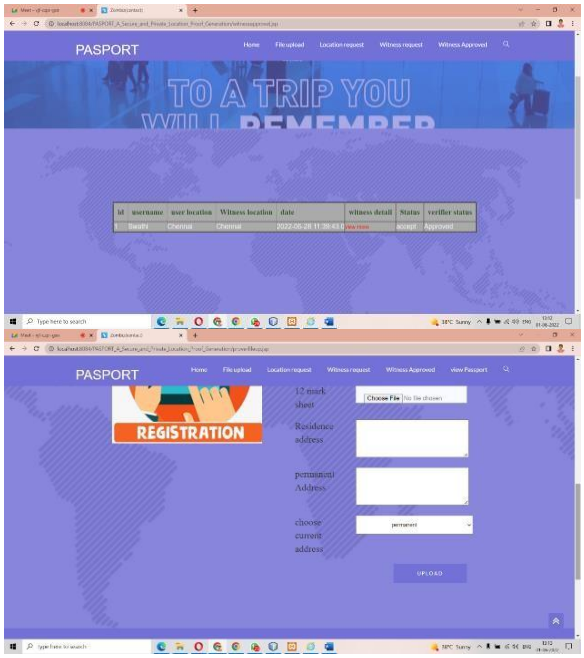

Fig. 6. File upload

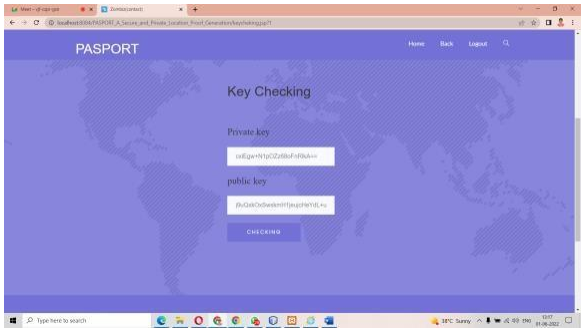

Fig. 7. Key checking

5. Conclusion

The proposed strategy's main advantages are that:

1) No strong centralized organization is required to act as a witness mechanism.
2) It has a dependable behavior against prover– prover and prover–witness collusions, to which the bulk of present schemes are subject.
3) Our new algorithm demonstrates that the proposed strategy's LP process is quicker than previous methods.
4) It protects users' privacy by allowing them to secretly publish their messages for local witnesses during the LP generation stage using the P-TREAD DB protocol. We can decrease our manual effort in our new system by using online passport verification. Only those who are permitted will receive approval from the verifier. Unauthorized individuals will be unable to obtain approval, and we will be able to conduct security by employing Identity-Based Broadcast Encryption technologies to protect our personal information.

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

[16] M. Grissa, A. A. Yavuz and B. Hamdaoui, "Location Privacy Preservation in Database-Driven Wireless Cognitive Networks Through Encrypted Probabilistic Data Structures," in IEEE Transactions on Cognitive Communications and Networking, vol. 3, no. 2, pp. 255-266, June 2017.

[17] K. Zeng, S. K. Ramesh, and Y. Yang, "Location spoofing attack and its countermeasures in database- driven cognitive radio networks," in Proc. IEEE Commun. Netw. Secur. (CNS), Oct. 2014, pp. 202–210.