ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

PASPORT: A SECURE AND PRIVATE LOCATION PROOF GENERATION AND VERIFICATION FRAMEWORK

Dr. ANIMONI NAGARAJU [1], AINOLLA CHANDI PRIYA (20S11A1212) [2], BUCHNOLA MANISHA (21S15A1203) [3], VELPULA ARAVIND (20S11A1208) [4], DHARMAVARAPU BHANU PRAKASH (20S11A1209) [5],

PROFESSOR AND HOD[1], UG STUDENTS [2,3,4,5,]

DEPARTMENT OF DATA SCIENCE AND INFORMATION TECHNOLOGY[1]

DEPARTMENT OF INFORMATION TECHNOLOGY [2,3,4,5,]

MALLA REDDY INSTITUTE OF TECHNOLOGY & SCIENCE,

Maisammaguda, Medchal (M), Hyderabad-500100, Telangana.

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 nontransferability 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.

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 activitytracking 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 3 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 . Now, we present some examples to highlight the relevant issues in these applications. 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 cangain unauthorized access to a system or resource by submitting fake location claims. In activitytracking 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. Thus far, with these examples, it is clear that preventing fake location submissions in these applications is still an open challenge. To protect these applications against location spoofing attacks, a number oflocation proof (LP) schemes have been proposed. Using these mechanisms, a mobile device (called a prover in the literature) receives one or more LPs from its neighbor devices when itvisits a site. The prover then submits the received LPs to the LBSP as a location claim. The LBSP checks the submitted LPs and either accepts or rejects the user's claim. LP schemes is categorized into two groups depending on the system architecture: centralized or distributed. In the centralized mechanisms , a trusted wireless infrastructure [such as a WiFi access point (AP)] is employed to generate LPs for mobile users. In distributed schemes , mobile users actas witnesses and generate LPs for each other. The latter approach is useful for scenarios in which there is no wireless infrastructure at the desired locations or it is expensive to employa large number of APs for different locations. In our extensive literature review and to the bestof our knowledge, we observed that all the current LP schemes suffer from at least one key drawback. First, some of these

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

schemes are vulnerable to prover–prover (P–P) collusions . In this attack, a remote malicious prover colludes with a dishonest user (located at a desired site)to obtain an LP. The dishonest user submits an LP request to the neighbor witness devices onbehalf of the remote prover. This security threat is called terrorist fraud in the literature . Second, none of the current distributed schemes offer a reliable solution for Prover–Witness (P–W) collusions. In this attack, a dishonest user acts as a witness for a remote malicious prover and generates a fake LP for him. Note that this security threat is specific to the distributed LP schemes only since witnesses are not trusted in this type of scheme. Finally, insome schemes, location privacy has not been considered , i.e., users broadcast their identity for neighbor devices or a third party server during the LP generation or submission process.

LITERATURE SURVEY

1. 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.[3] Today's location-sensitive service relies on user's mobile device to determine its location and send the location to the application. This approach allows the user to cheat by having his device transmit a fake location, which might enable the user to access a restricted resource erroneously or provide bogus alibis. To address this issue, we propose A Privacy-Preserving LocAtion proof Updating System in which co-located Bluetooth enabled mobile devices mutually generate location proofs, and update to a location proof server. 2. 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. [6] The proliferation of mobile devices has driven the mobile marketing to surge in the past few years. Emerging as a new type of mobile marketing, mobile location-based services (MLBSs) have attracted intense attention recently. Unfortunately, current MLBSs have a lot of limitations and raise many concerns, especially about system security and users' privacy. In this paper, we propose a new location-based rewarding system, called LocaWard, where mobile users can collect location-based tokens from token distributors, and then redeem their gathered tokens at token collectors for beneficial rewards. Tokens act as virtual currency. 3. van Cleeff, W. Pieters, and R. Wieringa, "Benefits of location-based access control: A literature study," in Proc. IEEE/ACM Int. Conf. Green Comput. Commun., Dec. 2010, pp. 739–746. [11] Activity-based social networks, where people upload and share information about their location-based activities (e.g., the routes of their activities), are increasingly popular. Such systems, however, raise privacy and security issues: the service providers know the exact locations of their users; the users can report fake location information to, for example, unduly brag about their performance. In this paper, we propose a secure privacy-preserving system for reporting location-based activity summaries (e.g., the total distance covered and the elevation gain). Our solution is based on a combination of cryptographic techniques and geometric algorithms, and 6 it relies on existing Wi-Fi access point networks deployed in urban areas.

Existing System

Existing schemes which require multiple trusted or semi-trusted third parties, STAMPrequires only Single semi-trusted third party which can be embedded in a Certificat Authority (CA). We design our system with an objective of protecting Users' anonymity and location privacy. No parties other than verifiers could see both a user's identity and STP information (verifiers need both identity and STP Information 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 type s of collusion attacks: (1) A user who is at an Intended location masquerades s 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 beenefforts to address this type of collusion. However, existing solutions suffer fromhigh 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. We Integrate the Bussard-Bagga distance bounding protocol into STAMP to protect our scheme against this collusion attack. Collusion scenario (1) is hard to prevent without a trusted third party. To make our system resilient to this attack, we propose an entropy-based trust model to detect the collusion scenario. We implemented STAMP on the Android platform and carried out extensive validation experiments. The experimental results show that STAMP requires low computational overhead.

Disadvantages of Existing System

Most of the existing STP proof schemes rely on wireless infrastructure (e.g., WiFi• APs) to create proofs for mobile users. However, it may not be feasible for all types of applications, e.g., STP proofs for the green commuting and

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

battlefield examples certainly cannot be obtained from wireless APs. Most ofthe existing schemes require multiple trusted or semi-trusted third parties.•

Proposed System

Motivated by this, to address these key concerns, we propose a distributed LP scheme, PrivacyAware and Secure Proof Of pRoximiTy (PASPORT), which performs LP generation and verification for mobile users in a secure and privacy-aware manner. The proposed scheme provides the integrity and nontransferablity of generated LPs. To make PASPORT resistant 2 to P–P collusions and perform private proximity checking, we develop a privacy-aware distance bounding (DB) protocol P-TREAD and integrate it into PASPORT. P-TREAD is a modified version of TREAD , a state of the art and secure DB protocol without privacy consideration. Our customization does not affect TREAD's main structure and features. Thus, PASPORT benefits from its security guarantees. By employing P-TREAD as the DB mechanism, a malicious prover colluding with an adversary can easily be impersonated by the adversary later. Generally, users do not take such a risk by initiating a prover–prover collusion. It has reliable performance against prover–prover and prover– witness collusions to which majority of the current schemes are vulnerable.our prototype implementation shows that LP generation process in the proposed scheme is faster than the existing schemes.

Advantages of Proposed System

No additional trusted third parties are required except for a semi-trusted CA.• STAMP requires only a single semi-trusted third party which can be embedded in• a Certificate Authority (CA). We design our system with an objective of protecting users' anonymity and• location privacy. No parties other than verifiers could see both a user's identity and STP information• (verifiers need both identity and STP information in order to perform verification provide services). A security analysis is presented to prove PASPORT achieves the security and• privacy objectives.

SYSTEM DESIGN

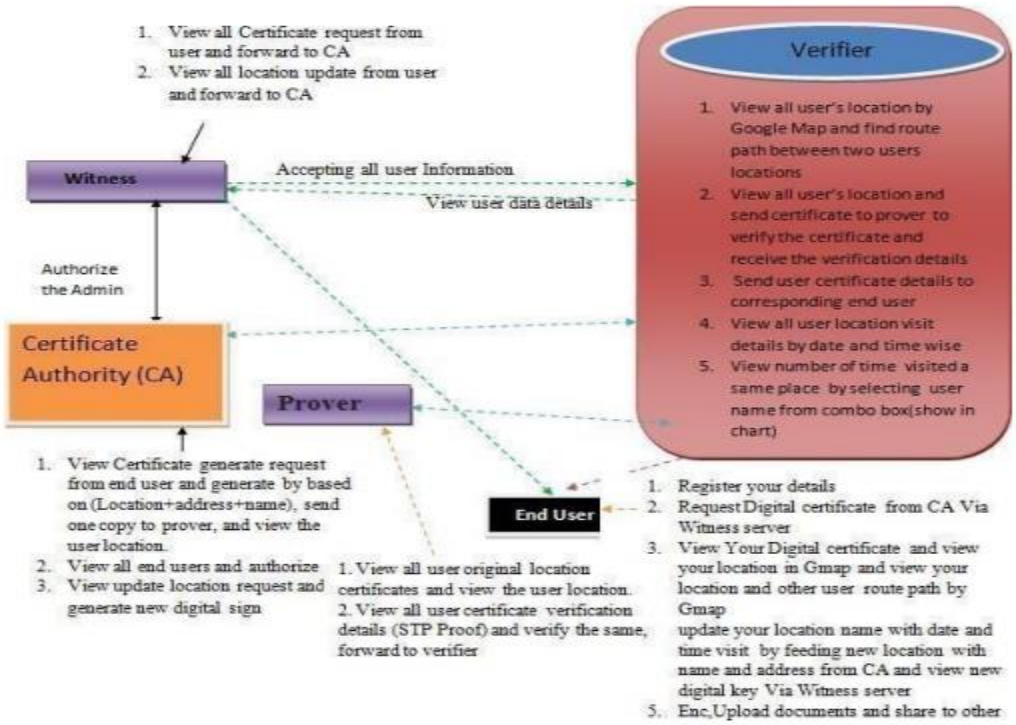


Figure.1 System architecture

Software Requirements

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

3.2.1.1 Operating System: Windows

3.2.1.2 Coding Language: JAVA

3.2.1.3 Backend: Html , JS

3.2.1.4 Database : SQLyog

3.2.1.5 API: JDBC

3.2.1.6 Server: Tomcat 6.0 Web Server

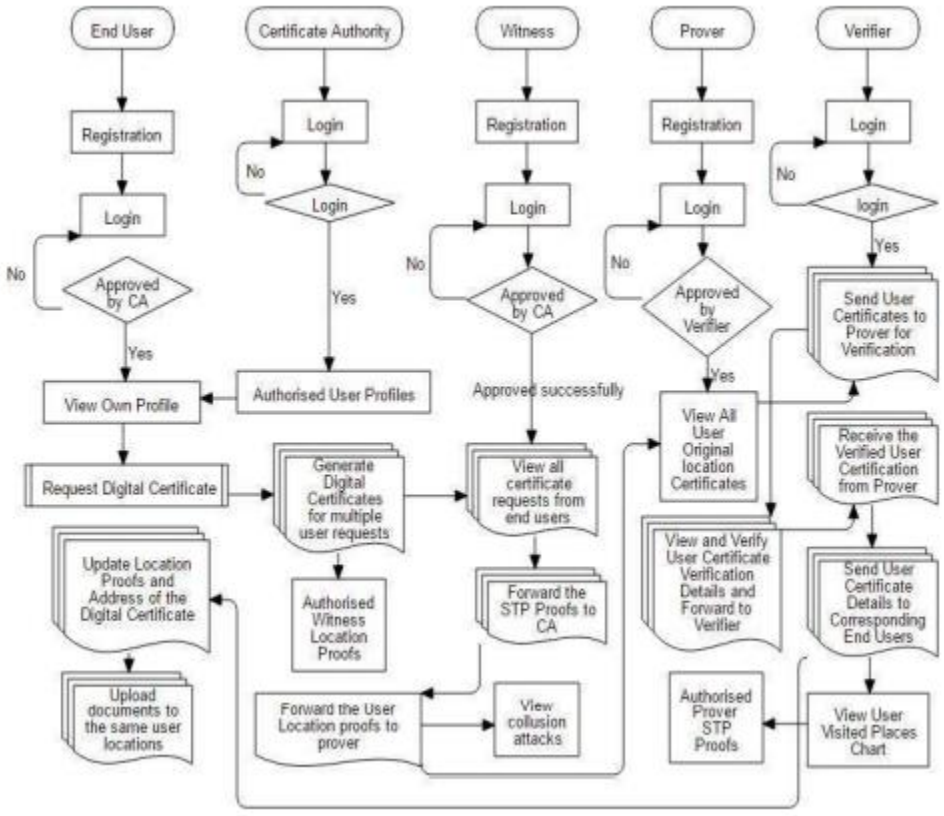
Hardware Requirements

3.2.2.1 Processor – intel core i5

3.2.2.2 RAM - 512 MB (min)

INPUT AND OUTPUT DESIGN

Input Design



Output Design

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Output for the above input will be displayed as digital certificate of the user which is to be sent to another user after verifying.

The certificate generation flow for the output is:

- User to Witness
- Witness to CA
- CA to verifier
- Verifier to Prover
- Prover to Verifier
- Verifier to User

RESULTS

Home page

Figure 2 Home page

Prover login

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Figure 3 Prover login

Prover authority

Figure 4 Prover authority

Verifier login

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Figure 5 Verifier login

Verifier authority

Figure 6 Verifier authority

Certification Authority login

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Figure 7 Certification authority login

Certification authority

Figure 8 Certification authority

Witness Authority

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Figure 9 Witness authority

User Registration

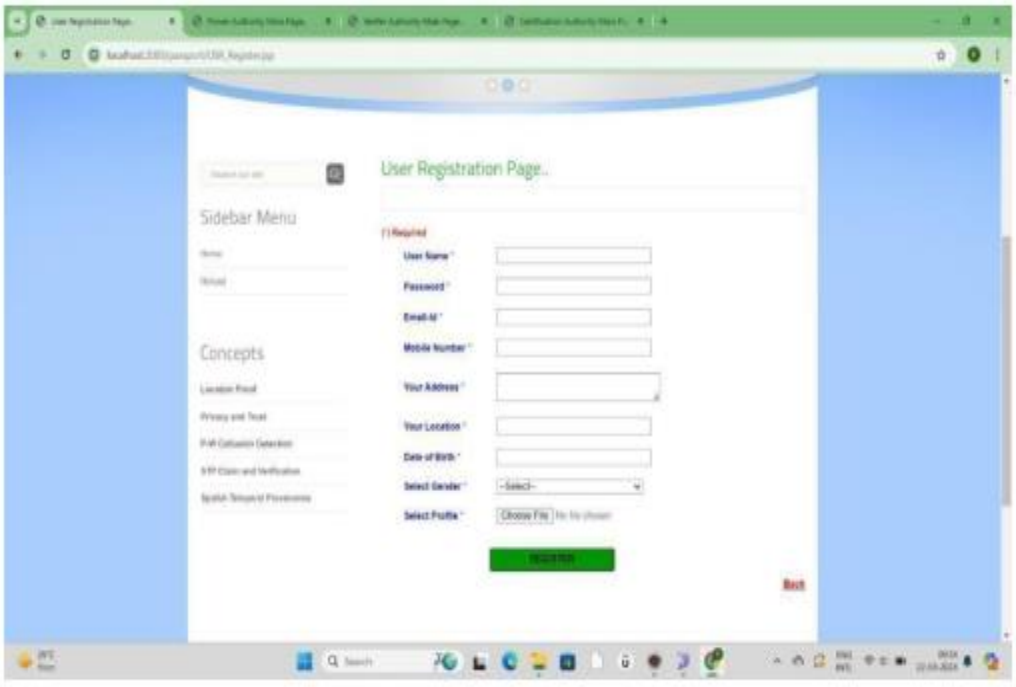


Figure 10 User registration

Welcome user

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

Figure 11 Welcome user

User profile

Figure 12 User profile

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 P-TREAD, 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 takessuch 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. The main strengths of the proposed scheme are: 1) no central trusted entity is required to operate as a witness device; 2) it has reliable performance against prover–

ISSN: 2278-4632
Vol-14 Issue-02 Aug 2024

prover and prover– witness collusions to which majority of the current schemes are vulnerable; 3) our prototype implementation shows that the LP generation process in the proposed scheme is faster than the existing schemes; and 4) it preserves users' location privacy as P-TREAD DB protocol enables users to anonymously broadcast their messages for the neighbor witnesses during the LP generation process. 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 blockchainbased incentive mechanism to encourage users to collaborate with the system can be another research direction for this article.

BIBLIOGRAPHY

[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. van Cleeff, W. Pieters, and R. Wieringa, "Benefits of location-based access control: A literature study," in Proc. IEEE/ACM Int. Conf. Green Comput. Commun., Dec. 2010, pp. 739–746. 41

[12] W. Luo and U. Hengartner, "VeriPlace: A privacy–aware location proof architecture," in Proc. ACM GIS, 2010, pp. 23–32.

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

[14] X. Wang, A. Pande, J. Zhu, and P. Mohapatra, "STAMP: Enabling privacy–preserving location proofs for mobile users," IEEE/ACM Trans. Netw., vol. 24, no. 6, pp. 3276–3289, Dec. 2016.

[15] B. Waters and E. Felten, "Secure, private proofs of location," Dept. Comput. Sci., Princeton Univ., Princeton, NJ, USA, Tech. Rep. TR–667–03, 2003.