

A Secure and Private Location Proof Generation and Verification Framework

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering

by

SADINENI BINDU NAIDU (Reg. No.40111089)

SANGEETHAM SATHWIK (Reg. No.40111130)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

CATEGORY-1 UNIVERSITY BY UGC

Accredited with Grade “A++” by NAAC | 12B Status by UGC | Approved by AICTE

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600119

APRIL - 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Category - I University by UGC

Accredited "A++" by NAAC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **SANGEETHAM SATHWIK** (Reg. No 40111130) and **SADINENI BINDU NAIDU** (Reg. No 40111089) who carried out the Project entitled "**A SECURE AND PRIVATE LOCATION PROOF GENERATION AND VERIFICATION FRAMEWORK**" under my supervision from November 2023 to April 2024.

Internal Guide

Dr. L. SUJHELEN, M.E., Ph.D.,

Head of the Department

Dr. L. LAKSHMANAN, M.E., Ph.D.,

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Jeppiaar Nagar, Rajiv Gandhi Salai,

Chennai - 600 119.

Submitted for Viva voce Examination held on

12/04/2024

Internal Examiner

External Examiner

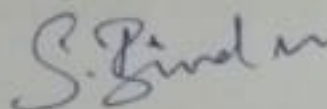
(Dr. P. Arko)

DECLARATION

I, SADINENI BINDU NAIDU (Reg. No 40111089) hereby declare that the Project Report entitled "A SECURE AND PRIVATE LOCATION PROOF GENERATION AND VERIFICATION FRAMEWORK" done by me under the guidance of Dr. L. SUJHELEN, M.E., Ph.D., is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **Computer Science and Engineering**.

DATE: 12/4/24

PLACE: Chennai



SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **The Board of Management of Sathyabama Institute of Science and Technology** for their encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. SASIKALA M.E., Ph. D, Dean, School of Computing, Dr. L. LAKSHMANAN M.E., Ph.D., Head of The Department,** Department of Computer Science and Engineering for providing me the necessary support the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. L. SUJHELEN, M.E., Ph. D,** for her valuable guidance, suggestions, and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

The rapid proliferation of location-based services (LBS) and the corresponding increase in location spoofing attacks have necessitated the development of robust and privacy-preserving location proof (LP) systems. The Privacy-Aware and Secure Proof Of pRoximiTy (PASPORT) scheme, presented in this paper, addresses the critical challenges faced by LBS providers by ensuring the authenticity of location claims while protecting user privacy. PASPORT introduces a decentralized architecture that leverages the ubiquity of mobile devices, allowing users to act as witnesses to generate LPs for each other in the absence of a trusted wireless infrastructure. This paper delineates the design and implementation of PASPORT, which incorporates a privacy-aware distance bounding (DB) protocol, P-TREAD, to resist prover-prover and prover-witness collusion attacks effectively. The PASPORT scheme is meticulously crafted to provide integrity and nontransferability of LPs, ensuring that location proofs cannot be forged or repurposed by malicious entities. The integration of P-TREAD, a modified version of the state-of-the-art TREAD protocol, enhances the security of the proximity checking process without compromising privacy. The scheme's resilience to collusion attacks is achieved through a novel witness selection mechanism and an entropy-based trust model, which collectively reduces the success probability of such attacks to a negligible value. Extensive experiments conducted on the Android platform demonstrate that PASPORT outperforms existing distributed LP schemes in terms of computational efficiency and response time. The scheme's practicality is further evidenced by its low computational resource requirements and its ability to operate effectively in both indoor and outdoor environments. The paper also provides a comprehensive security and privacy analysis, confirming that PASPORT achieves the necessary security properties, including resistance to distance frauds, unforgeability, nontransferability, and resistance to various collusion and hijacking attacks. The PASPORT scheme's usability is enhanced by the inclusion of an incentive mechanism that encourages user participation, ensuring a sufficient number of witnesses for LP generation.

TABLE OF CONTENTS

Chapter No	TITLE	Page No.
	ABSTRACT	v
	LIST OF FIGURES	viii
1	INTRODUCTION	1
2	LITERATURE SURVEY	4
3	REQUIREMENT ANALYSIS	9
	3.1 DRAWBACKS OF EXISTING SYSTEMS	9
	3.2 PROPOSED SYSTEM	9
	3.3 SYSTEM REQUIREMENTS	10
	3.3.1 HARDWARE REQUIREMENTS	10
	3.3.2 SOFTWARE REQUIREMENTS	11
4	DESCRIPTION OF PROPOSED SYSTEM	12
	4.1 PROPOSED WORK	12
	4.2 ARCHITECTURE DIAGRAM	13
	4.3 A SCHEMATIC DIAGRAM OF A LOCATION SYSTEM	13
	4.3.1 PROVER	14
	4.3.2 WITNESS	14
	4.3.3 VERIFIER	14
	4.4 TRUST AND THREAT MODEL	16
	4.4.1 TRUST MODEL	16
	4.4.2 THREAT MODEL	16
5	SYSTEM IMPLEMENTATION	18
	5.1 HOME PAGE	18
	5.2 PROVER PAGE	18
	5.3 VERIFIER MODULE	19
	5.3.1 PROVER REQUESTS MODULE	20

5.3.2	LOCATION REQUESTS MODULE	21
5.3.3	UPLOAD DATA MODULE	21
5.3.4	REJECTED USERS MODULE	22
5.3.5	USER RATINGS MODULE	22
5.3.6	LOGOUT FUNCTIONALITY	22
6	RESULTS AND DISSCUSION	23
6.1	VERIFICATION OF GENUINE LOCATION CLAIMS	23
6.2	USER ACCESS TO LOCATION-BASED SERVICES	23
6.3	SYSTEM PERFORMANCE AND EFFICIENCY	25
6.4	PRIVACY PRESERVATION	25
6.5	SECURITY AND RELIABILITY	25
7	CONCLUSION	26
7.1	CONCLUSION	26
7.2	FUTURE ENHANCEMENTS	27
	REFERENCES	28
	APPENDIX	30
A	SOURCE CODE	30

LIST OF FIGURES

FIGURE NO	FIGURE NAME	Page No.
4.1	ARCHITECTURE DIAGRAM	13
4.2	PROVER FLOW DIAGRAM	15
4.3	VERIFIER FLOW DIAGRAM	15
4.4	MESSAGE EXCHANGE DIAGRAM FOR THE PROPOSED SCHEME	17
5.1	HOME PAGE	18
5.2	PROVER MODULE	19
5.3	VERIFIER CONSOLE	20
5.4	PROVER REQUESTS	20
5.5	UPLOAD DATA	21
5.6	REJECTED USERS	22
6.1	USER ACCESSING LB SERVICES	24
6.2	GENIUNE USER RATINGS	24

LIST OF TABLES

TABLE NO	TABLE NAME	PAGE NO.
2.1	Literature Survey	7

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

The project "Privacy-Aware and Secure Proof Of pRoximiTy" (PASPORT) addresses the critical issue of fake location submissions in location-based systems and applications. These systems, which are increasingly popular, are vulnerable to location spoofing attacks where dishonest users submit false location information to gain access to services, resources, or rewards. The consequences of such fraudulent activities can be severe, undermining the integrity of these applications and violating user privacy. PASPORT proposes a decentralized architecture that allows mobile users to generate and verify location proofs (LPs) for each other in an ad hoc manner, enhancing security and privacy. This framework ensures that LPs are unforgeable and non-transferable, making it difficult for users to cheat the system. Additionally, PASPORT is designed to be resilient against collusion attacks, including both prover-prover and prover-witness collusions, which are significant threats to distributed LP schemes. To further enhance privacy, PASPORT integrates a privacy-aware distance bounding protocol called P-TREAD. This protocol ensures that the process of proximity checking does not compromise user privacy. The PASPORT scheme has been validated through a prototype implementation on the Android platform, and extensive experiments indicate that it can efficiently protect location-based applications against fake submissions. The PASPORT project represents a significant advancement in securing location-based services. It not only provides a robust mechanism for generating and verifying location proofs but also prioritizes user privacy, ensuring that sensitive location information is not exposed to service providers or other unauthorized parties. By addressing both security and privacy concerns, PASPORT offers a promising solution for the future of location-based applications.

1.2 PURPOSE OF THE PASPORT PROJECT

The purpose of the PASPORT (Privacy-Aware and Secure Proof Of pRoximiTy) project is to develop a secure and privacy-aware framework for generating and verifying

location proofs (LPs) in location-based systems and applications. This project aims to address the critical issue of fake location submissions, which can have severe consequences for the integrity and reliability of location-based services (LBSs). The PASPORT scheme is designed to ensure that users submit a true and verifiable LP to service providers, thereby preventing dishonest users from cheating on their location to gain unauthorized access to services, resources, or rewards. The PASPORT project introduces a decentralized architecture suitable for ad hoc scenarios, where mobile users can act as witnesses to generate LPs for each other. This approach enhances user privacy protection and provides security properties such as unforgeability and non-transferability of LPs. Additionally, the PASPORT scheme incorporates a privacy-aware distance bounding protocol, P-TREAD, to further secure the proximity checking process and make it private. By implementing the PASPORT framework, the project seeks to protect SBSs against location spoofing attacks, reduce the success probability of Prover-Witness collusion attacks, and ensure user privacy during the LP generation and verification process. The ultimate goal is to create a robust system that can efficiently protect location-based applications from fake submissions while maintaining user privacy and trust.

1.3 PROBLEM STATEMENT

The rapid expansion of location-based systems and applications has led to a surge in the need for users to submit accurate location information to service providers to access services, resources, or rewards. However, these systems are currently plagued by the vulnerability of location spoofing attacks, where dishonest users falsify their location data to gain undue advantages. This critical issue not only undermines the integrity of location-based services (LBSs) but also poses severe consequences for their reliability and the trust of their users. The existing mechanisms for location proof (LP) generation and verification are insufficiently equipped to combat fake location submissions effectively. Centralized LP schemes rely on trusted wireless infrastructure, which is not always available or economically feasible to deploy extensively. On the other hand, distributed LP schemes, which allow mobile users to act as witnesses for each other, are susceptible to Prover-Witness and Prover-Prover collusion attacks,

where dishonest users and witnesses conspire to generate fraudulent LPs. Furthermore, the current LP schemes do not adequately protect user privacy during the LP generation or submission process, often requiring users to broadcast their identity to neighbor devices or third-party servers. Additionally, these schemes suffer from high communication and computation overheads and expensive implementation costs, making them impractical for widespread adoption.

1.4 OBJECTIVES

The objective of the PASPORT (Privacy-Aware and Secure Proof Of pRoximiTy) project is to develop a secure and privacy-aware framework for generating and verifying location proofs (LPs) in location-based systems and applications. This project aims to address the critical issue of fake location submissions, which can undermine the integrity and reliability of location-based services (LBSs). By introducing a decentralized architecture suitable for ad hoc scenarios, the PASPORT project seeks to enable mobile users to act as witnesses for each other, generating LPs that are unforgeable, non-transferable, and resilient to collusion attacks. Furthermore, the integration of the P-TREAD protocol, a privacy-aware distance bounding protocol, into the PASPORT scheme aims to enhance the security and privacy of the proximity checking process. Ultimately, the project's goal is to protect SBSs against location spoofing attacks, reduce the success probability of collusion attacks to a negligible level, and ensure user privacy during the LP generation and verification process.

CHAPTER 2

LITERATURE SURVEY

1) Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges, and countermeasures

AUTHORS: P. Asuquo et al

Location-based services (LBSs) have gained popularity as a result of the advances in mobile and communication technologies. LBS provide users with relevant information based on their location. In spite of the desirable features provided by LBS, the geographic locations of users are not adequately protected. Location privacy is one of the major challenges in vehicular and mobile networks. In this paper, we analyze the security and privacy requirements for LBS in vehicular and mobile networks. Specifically, this paper covers privacy enhancing technologies and cryptographic approaches that provide location privacy in vehicular and mobile networks. The different approaches proposed in literature are compared and open research areas are identified.

2) A survey of fingerprint-based outdoor localization

AUTHORS: Q. D. Vo and P. De

A growing number of sensors on smart mobile devices has led to rapid development of various mobile applications using location-based or context-aware services. Typically, outdoor localization techniques have relied on GPS or on cellular infrastructure support. While GPS gives high positioning accuracy, it can quickly deplete the battery on the device. On the other hand, base station based localization has low accuracy. In search of alternative techniques for outdoor localization, several approaches have explored the use of data gathered from other available sensors, like accelerometer, microphone, compass, and even daily patterns of usage, to identify unique signatures that can locate a device. Signatures, or fingerprints of an area, are hidden cues existing around a user's environment. However, under different operating scenarios, fingerprint-based localization techniques have variable performance in terms of accuracy, latency of

detection, battery usage. The main contribution of this survey is to present a classification of existing fingerprint-based localization approaches which intelligently sense and match different clues from the environment for location identification. We describe how each fingerprinting technique works, followed by a review of the merits and demerits of the systems built based on these techniques. We conclude by identifying several improvements and application domain for fingerprinting based localization.

3) An exploration to location-based service and its privacy preserving techniques: A survey

AUTHORS: R. Gupta and U. P. Rao

Mobile gadgets today are swaggering computing potential and memory at par or at times even higher to that found in desktop personal computers. A wireless interconnection has turned out to be considerably more readily accessible these days. As individuals are growing mobile with regard to the fast lifestyle and working pattern, a new, smarter system came into existence that is termed as 'Location Based Service' (LBS). Such a system amalgamates the location data of a user with smart applications to deliver demanded services. Although LBS provide major openings for a large variety of markets and remarkable convenience to the end user, it also presents subtle privacy attack to user's location information. Threat to the privacy sneaks into the system due to the prerequisite of sending user's current location to the LBS provider to attain related services. Since the volume of data gathered from dynamic or stationary mobile users using LBS can be high, it is vital to outline the frameworks and systems in a manner that is secure and keep the location information private. In this paper, we perform an exploratory survey about the various techniques that have been suggested by many researchers based on centralized and distributed approaches, to preserve location privacy of the user. A large portion of these techniques has a trade-off between privacy, efficiency, applicability and quality of service. This paper details and analyses the various existing techniques for preserving location privacy of the participating user in LBS.

4) Location based handshake and private proximity test with location tags

AUTHORS: Y. Zheng, M. Li, W. Lou, and Y. T. Hou

A location proximity test service allows mobile users to determine whether they are in close proximity to each other, and has found numerous applications in mobile social networks. Unfortunately, existing solutions usually reveal much of users' private location information during a proximity test. They are also vulnerable to location cheating where an attacker reports false locations to gain an advantage. Moreover, the initial trust establishment among unfamiliar users in large scale mobile social networks has been a challenging task. In this paper, we propose a novel scheme that enables a user to perform (1) a location based handshake that establishes secure communications among strangers, who do not have a pre-shared secret, and (2) a privacy-preserving proximity test without revealing the user's actual location to the server or other users not within the proximity. The proposed scheme is based on a novel concept, i.e., spatial-temporal location tags, and we put forward a location tag construction method using environmental signals that provides an unforgeable location proof. We use Bloom filters to efficiently represent users' location tags and vicinity regions. We exploit fuzzy extractor, a lightweight cryptographic primitive, to extract shared secrets between matching location tags. We conduct extensive analysis, simulation, and real experiments to demonstrate the feasibility, security, and efficiency of our scheme.

5) Privacy-preserving location proof for securing large-scale database-driven cognitive radio networks

AUTHORS: Y. Li, L. Zhou, H. Zhu, and L. Sun

The latest Federal Communications Commission (FCC) ruling has enforced database-driven cognitive radio networks (CRNs), in which all secondary users (SUs) can query a database to obtain spectrum availability information (SAI). Database-driven CRNs are regarded as a promising approach for dynamic and highly efficient spectrum management paradigm for large-scale Internet of Things (IoT). However, as a typical location-based service (LBS), before providing services to the user, there is no

verification of the queried location, which is very vulnerable to location spoofing attack. A malicious user can report a fake location to the database and access the channels that may not be available for its location. This will introduce serious interference to the primary users (PUs). In this study, we identify a new kind of attack coined as location cheating attack, which allows an attacker to spoof other users to another location and make them query the database with wrong location, or allows a malicious user to forge location arbitrarily and query the database for services. To thwart this attack, we propose a novel infrastructure-based approach that relies on the existing WiFi or cellular network access points (or AP) to provide privacy-preserving location proof. With the proposed solution, the database can verify the locations without knowing the user's accurate location. We perform comprehensive experiments to evaluate the performance of the proposed approach.

S.NO	TITLE	AUTHOR/YEAR	RESULTS	TECHNIQUE
1	Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges, and countermeasures	Philip Asuquo , Haitham Cruickshank/ 2018	In this article, we analyse the security and privacy requirements for LBS in vehicular and mobile networks. Specifically, this paper covers privacy enhancing technologies and cryptographic approaches that provide location privacy in vehicular and mobile networks. The different approaches proposed in literature are compared and open research areas are identified.	A hybrid approach for private location-based query is proposed by. This approach protects the user and the LBS database. They provide a strong privacy by generalizing the user location to coarse-grained cloaked regions and apply a PIR protocol to the queries from the cloaked region.

S.NO	TITLE	AUTHOR/YEAR	RESULTS	TECHNIQUE
2	A survey of fingerprint-based outdoor localization	Quoc Duy Vo/ 2019	The main contribution of this survey is to present a classification of existing fingerprint-based localization approaches which intelligently sense and match different clues from the environment for location identification. We describe how each fingerprinting technique works, followed by a review of the merits and demerits of the systems built based on these techniques. We conclude by identifying several improvements and application domain for fingerprinting based localization.	Typically, outdoor localization techniques have relied on GPS, or on cellular infrastructure support. While GPS gives high positioning accuracy, it can quickly deplete the battery on the device

S.NO	TITLE	AUTHOR/YEAR	RESULTS	TECHNIQUE
3	An exploration to location-based service and its privacy preserving techniques: A survey	R. Gupta and U. P. Rao/2017	In this paper, we perform an exploratory survey about the various techniques that have been suggested by many researchers based on centralized and distributed approaches, to preserve location privacy of the user. A large portion of these techniques has a trade-off between privacy, efficiency, applicability and quality of service. This paper details and analyses the various existing techniques for preserving location privacy of the participating user in LBS.	Here we use cloaking algorithm.

Table 2.1 Literature Survey

CHAPTER 3

REQUIREMENT ANALYSIS

3.1 DRAWBACKS OF EXISTING SYSTEMS

- Saroiu and Wolman proposed a technique in which the AP broadcasts beacon frames consisting 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.
- APPLAUS introduced by Zhu and Cao is one of the pioneer research works on distributed LP systems. In APPLAUS, mobile devices use their short range Bluetooth interface to communicate with their nearby devices who request an LP. To preserve users' location privacy, they need to select a set of M pseudonyms and change them periodically. These pseudonyms are considered as users' public keys, which are required to be registered with a trusted certificate authority (CA) along with the associated private keys. However, changing pseudonyms regularly creates a high level of computation and communication overhead.

3.2 PROPOSED SYSTEM

- We propose a distributed LP scheme, Privacy-Aware 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 non-transferability of generated LPs. To make PASPORT resistant 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.

- We design PASPORT, a secure, privacy-aware and collusion-resistant LP scheme for mobile users. PASPORT has a decentralized architecture suitable for scenarios in which a fixed wireless infrastructure does not exist. To privately perform the procedure of proximity checking, we propose P-TREAD, a privacy-aware and secure DB mechanism and integrate it into PASPORT.

3.3 SYSTEM REQUIREMENTS

The PASPORT (Privacy-Aware and Secure Proof Of pRoximiTy) project aims to enhance the security and privacy of location-based services through a decentralized architecture and the integration of a privacy-aware distance bounding protocol. To successfully implement and operate the PASPORT framework, specific system requirements must be established. These requirements encompass both hardware and software components necessary for the deployment and functionality of the PASPORT scheme.

3.3.1 HARDWARE REQUIREMENTS

- System Processor: Pentium i5 Processor, ensuring efficient processing and multitasking capabilities.
- Hard Disk: 500 GB SSD, offering fast data access and storage solutions.
- Monitor: 15" LED, providing clear and vibrant display quality for user interaction.
- Input Devices: Keyboard and Mouse, facilitating easy and intuitive system navigation and data input.
- RAM: 8 GB, supporting smooth operation and sufficient memory for running multiple applications simultaneously.

3.3.2 SOFTWARE REQUIREMENTS

- Operating System: Windows 11, offering the latest security features and support for modern applications.
- Coding Language: JAVA, chosen for its portability, object-oriented features, and extensive library support.
- Tool: NetBeans 8.2, providing a powerful integrated development environment (IDE) for efficient coding, debugging, and testing of JAVA applications.
- Database: MYSQL, selected for its reliability, scalability, and support for complex data structures, ensuring robust data management and retrieval.
- Encryption Algorithm: The PASPORT scheme employs the Triple DES algorithm for encrypting location data. This choice ensures the confidentiality, integrity, and authenticity of the data transmitted within the system. The Triple DES algorithm is known for its robust security features, making it suitable for protecting sensitive location information against unauthorized access and manipulation.
- Development Technologies: The user interface and user experience design for the PASPORT application are developed using a combination of JavaScript, HTML, and CSS. These technologies are chosen for their flexibility and wide support across various platforms, ensuring an intuitive and responsive design. The use of JavaScript allows for dynamic content and interactive features, while HTML and CSS provide the structure and style of the application interface.

CHAPTER 4

DESCRIPTION OF PROPOSED SYSTEM

4.1 PROPOSED WORK

The envisioned framework, "A Secure and Private Location Proof Generation and Verification Framework," seeks to establish a robust solution to the pervasive issue of location spoofing in location-based services. This initiative is driven by the need to authenticate the veracity of location claims, thereby ensuring the integrity of services that rely on accurate user location data. At the heart of this initiative is the creation of a decentralized system that enables mobile users to mutually verify their locations without the need for a centralized authority. This peer-to-peer verification model is designed to empower users to act as both provers and witnesses within the network, thus fostering a collaborative environment for location proofing. To enhance the privacy and security of the location verification process, the framework will incorporate a novel protocol, P-TREAD, which is a privacy-aware distance bounding protocol. This protocol is a critical component of the system, ensuring that the location proofs are not only secure against collusion and other forms of attacks but also preserve the anonymity of the users involved. The system will be rigorously tested through a prototype implementation on the Android platform, which will serve as a tangible demonstration of the framework's capabilities. This prototype will undergo extensive testing to evaluate its performance in terms of speed, resource consumption, and resilience to security threats. In addition to the core functionality, the framework will explore the integration of advanced features such as location granularity control, allowing users to determine the precision of their location data shared with the services. Furthermore, the potential for a blockchain-based incentive mechanism will be investigated to encourage user participation and cooperation in the location proofing process. This comprehensive approach aims to deliver a solution that not only addresses the current challenges faced by location-based services but also sets a new standard for privacy and security in the verification of location data. Through this work, the framework aspires to enhance the trustworthiness and reliability of location-based applications, ultimately benefiting both service providers and users alike.

4.2 ARCHITECTURE DIAGRAM

The following diagram illustrates the architecture of the proposed model:

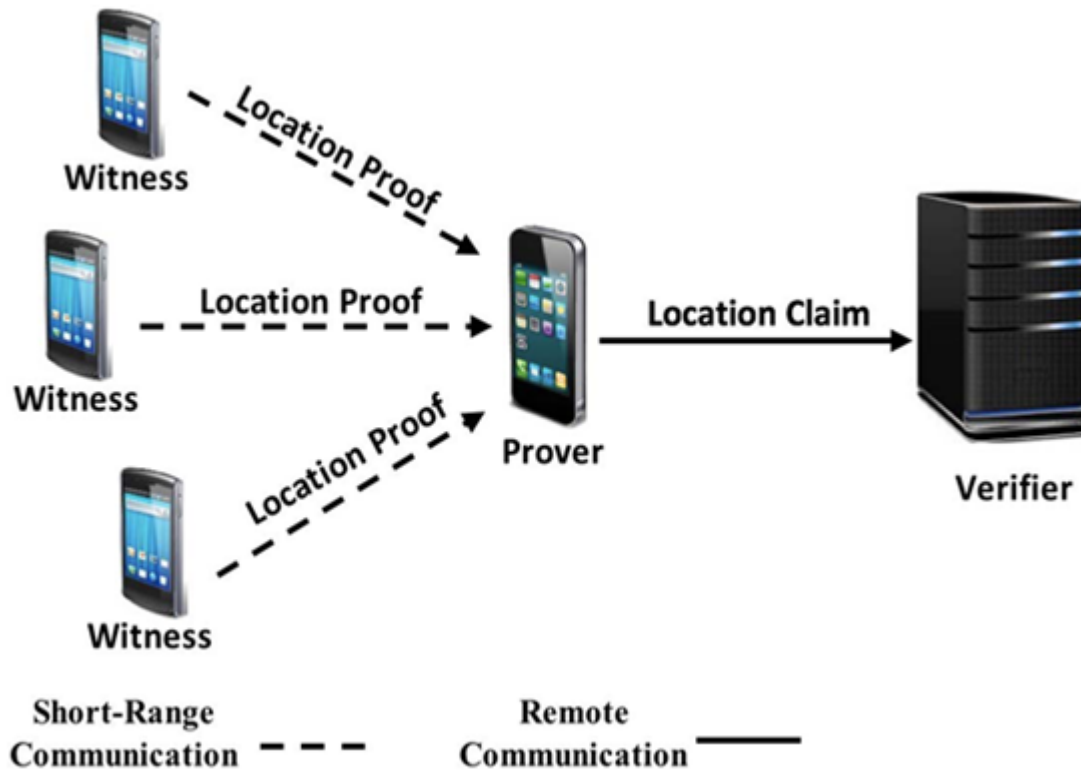


Fig:4.1 Architecture Diagram

4.3 A SCHEMATIC DIAGRAM OF A LOCATION PROOFING SYSTEM

The system architecture of the PASPORT project is designed to facilitate a secure and decentralized method for location proof generation and verification, which is particularly well-suited for ad hoc scenarios. This architecture eliminates the need for a centralized trusted entity, instead relying on the collaboration between users within the system. Here's a detailed elaboration of the three key roles within this architecture:

4.3.1 PROVER

The prover is a mobile user who requires verification of their physical location in order to access specific services or resources. The prover initiates the process by broadcasting a request for a location proof (LP) when they are at the desired location. The prover's device is equipped with the necessary technology to communicate with other users' devices in the vicinity to facilitate the generation of an LP.

4.3.2 WITNESS

Witnesses are other mobile users who are physically present in the same location as the prover and can attest to the prover's claim. These users receive the prover's request and, upon confirmation of the prover's presence, generate an LP. The LP is a cryptographic assertion that serves as evidence of the prover's location. Witnesses play a crucial role in the decentralized architecture, as they provide the necessary corroboration for the prover's location claim without the involvement of a centralized authority.

4.3.3 VERIFIER

The verifier is an entity, typically authorized by the service provider, that is responsible for verifying the LPs submitted by provers. Once the prover has collected LPs from one or more witnesses, they compile these into a location claim and submit it to the verifier. The verifier then examines the submitted LPs to authenticate their validity. This process involves checking the cryptographic signatures of the witnesses and ensuring that the LPs collectively confirm the prover's location claim. If the LPs are verified to be authentic and accurate, the verifier accepts the location claim; otherwise, it is rejected. The architecture depicted in the diagram ensures that the entire process, from LP generation to verification, is secure and privacy-preserving. The use of short-range communication between the prover and witnesses for LP generation, followed by remote communication to submit the location claim to the verifier, provides a layered approach to security. This design not only protects against common threats such as collusion and spoofing but also maintains the privacy of the users by not disclosing their identities beyond the necessary scope.

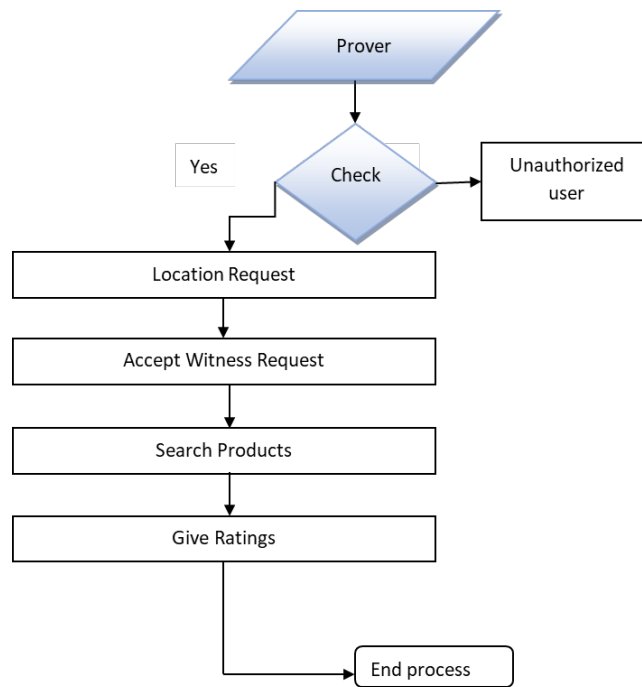


Fig:4.2 Prover Flow Diagram

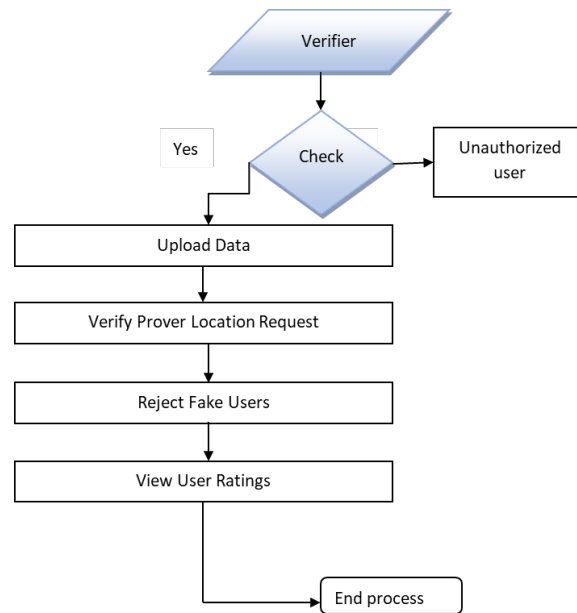


Fig:4.3 Verifier Flow Diagram

4.4 TRUST AND THREAT MODEL

4.4.1 TRUST MODEL

The trust model for the PASPORT system is built on the premise that all users, referred to as provers, are registered with a service provider. Each prover is assigned a unique public-private key pair, which is certified by a Certificate Authority (CA). This certification process is crucial for establishing trust within the system, as it ensures that each user's identity can be authenticated and verified through their public key. The private key, which is kept secret by the user, is used to sign location proofs (LPs) and other sensitive transactions to maintain integrity and non-repudiation

The trust model also assumes that users will not share their private keys with others, as doing so would compromise their security and the overall trustworthiness of the system. This is an important consideration, especially in scenarios where collusion might occur. The model relies on the assumption that even in collusion scenarios, a malicious prover would not go to the extent of providing their private key to another party

4.4.2 THREAT MODEL

The threat model for PASPORT addresses various potential attacks that could compromise the integrity and reliability of the location proof generation and verification process. Two primary types of collusion attacks are considered:

1. **Prover-Prover Collusions (Terrorist Frauds):** This type of attack involves collusion between a remote malicious prover and a dishonest user who is physically present at the desired location. The dishonest user submits an LP request to the neighboring witness devices on behalf of the remote prover. This type of attack is also known as a terrorist fraud in the literature. The PASPORT system is designed to be resilient against such attacks by ensuring that LPs cannot be generated without the prover's actual presence at the location¹.
2. **Prover-Witness Collusions:** In this scenario, a dishonest user acts as a witness and colludes with a remote malicious prover to generate a fake LP for them. The threat model takes into account the possibility of such collusion and implements

measures to significantly reduce the success probability of these attacks. The system ensures that it is not feasible for a malicious prover to create an LP without proving their location to a qualified witness1.

The threat model also considers the privacy of users, ensuring that their identities are not broadcasted during the LP generation or submission process. This is achieved through anonymous communication channels, such as Wi-Fi or Bluetooth, which allow users to broadcast messages without revealing identifying data like IP or MAC addresses.

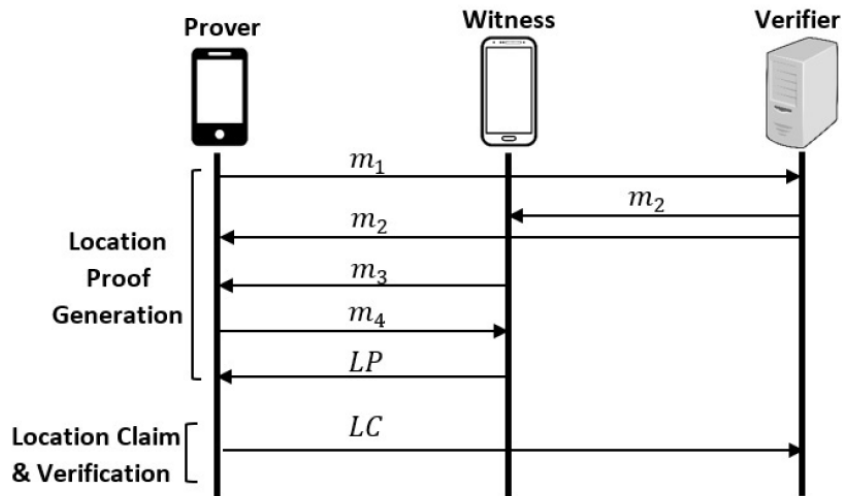


Fig:4.4 Message exchange diagram for the proposed scheme.

CHAPTER 5

SYSTEM IMPLEMENTATION

The system implementation for this project involves a structured approach to facilitate the interaction between provers and verifiers. The implementation is designed to ensure a seamless user experience while maintaining the integrity and security of the location proofing process. Below are the detailed steps for the system implementation:

5.1 Home Page

The home page serves as the entry point for both provers and verifiers. It is designed to be intuitive and user-friendly, providing clear navigation to the respective functionalities for each role.

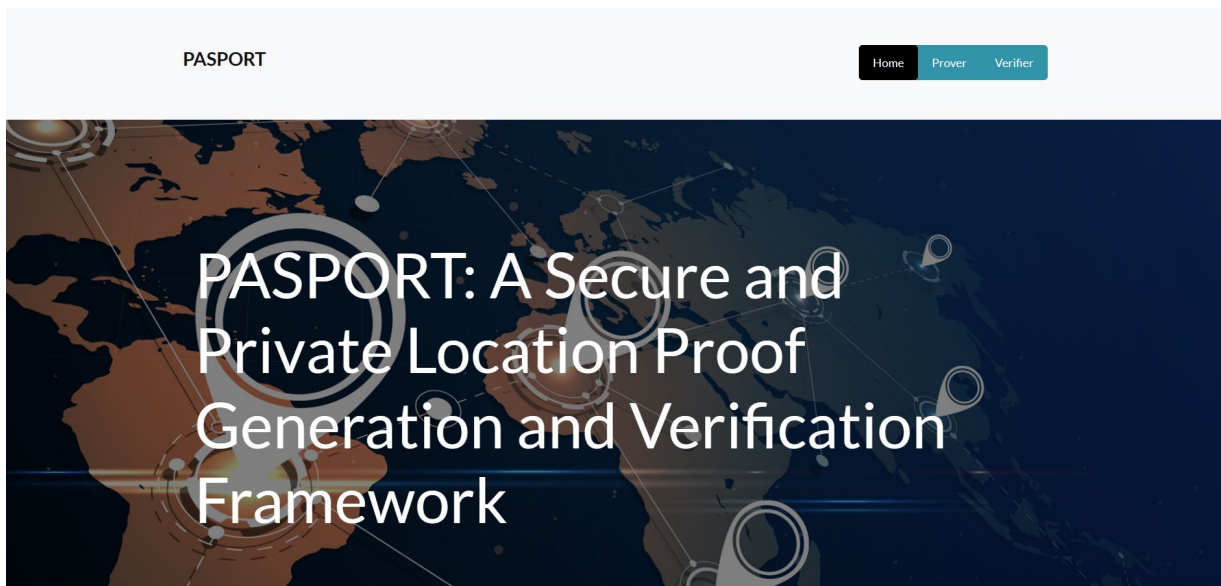


Fig:5.1 HOME PAGE

5.2 Prover Page

1. **User Login:** The prover page features a secure login mechanism. Users are required to log in using their credentials. For new users, there is an option to register.

2. **User Registration:** New users can register by providing the necessary information. The registration form is designed to capture essential details while ensuring user privacy.
3. **Verifier Approval:** Once a new user has registered, their account is subject to approval by the verifier. This step is crucial to maintain the system's integrity and prevent unauthorized access.
4. **Access to Services:** After receiving approval from the verifier, users can log in and access the services offered by the system, such as submitting location proofs to gain access to location-based services.

PASPORT

HomeProverVerifier

User Login



Email :

Enter Email ID

Password :

Enter Password

LOGINREGISTER

Fig:5.2 PROVER MODULE

5.3 Verifier Module

The verifier console is a critical component of the PASPORT project's system architecture, serving as the central hub for managing and overseeing the entire location proofing process. It is designed to be a comprehensive and secure interface that allows the verifier to execute a variety of tasks essential to the operation of the system. Here is an elaboration on the various modules and functionalities of the verifier console:

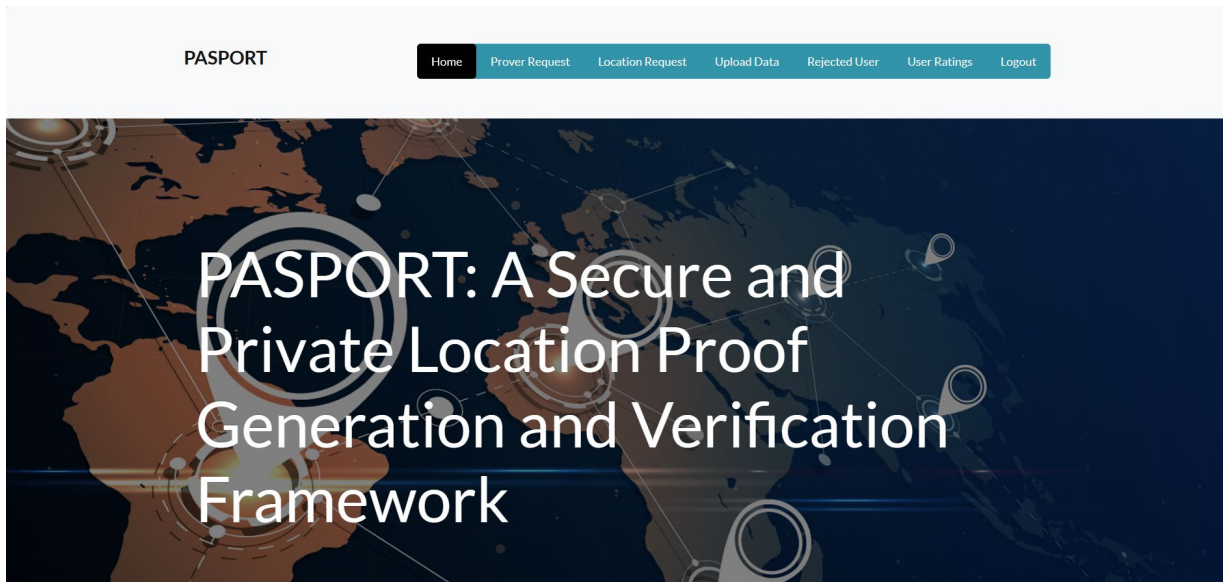


Fig:5.3 VERIFIER CONSOLE

5.3.1 Prover Requests Module

This module is the gateway for new users to join the system. It lists all the registration requests submitted by users who wish to become provers. The verifier is responsible for reviewing these requests to ensure that only legitimate users are granted access to the system. Once a user is approved, they are granted the status of a prover and can begin using the location-based services offered by the system.

PASPORT				
Home Prover Request Location Request Upload Data Rejected User User Ratings Logout				
Prover Requests				
Prover Name	Mail ID	Verify Key	Status	Action
abdul	abdulhathi@gmail.com	Y0lhWBHGR9iJJSpQl9fUJg==	Approved	Approve
santosh	sonsandy1993@gmail.com	KXAsa2rHe3aJJSpQl9fUJg==	Approved	Approve
sathwiktest	sathwik@gmail.com	DCfrNXj4LpmJJSpQl9fUJg==	Approved	Approve
Test1	Test1@gmail.com	CJpJT1CtiBaJJSpQl9fUJg==	Approved	Approve

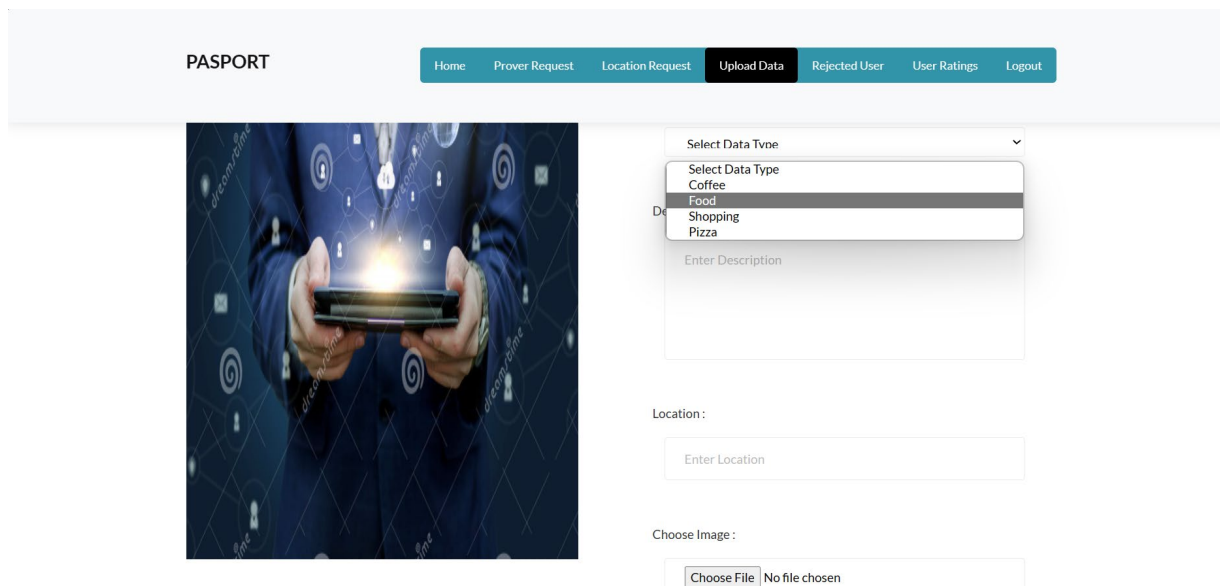
Fig:5.4 PROVER REQUESTS

5.3.2 Location Requests Module

In this section, the verifier receives and processes requests from provers who need to authenticate their physical location to access specific services. These location proof requests are critical for maintaining the integrity of location-based services, as they ensure that only users who are physically present at a given location can access the service or resource. The verifier evaluates the location proofs submitted by the provers, which have been corroborated by witnesses, to determine the authenticity of the location claims.

5.3.3 Upload Data Module

The upload data module allows the verifier to introduce new data into the system, which is pertinent to the services being offered. For instance, if the system is utilized for product ratings, the verifier can upload detailed information about new products. This data is then made available to provers who, upon successful location verification, can provide ratings. This module is essential for keeping the service content up-to-date and relevant to the users.

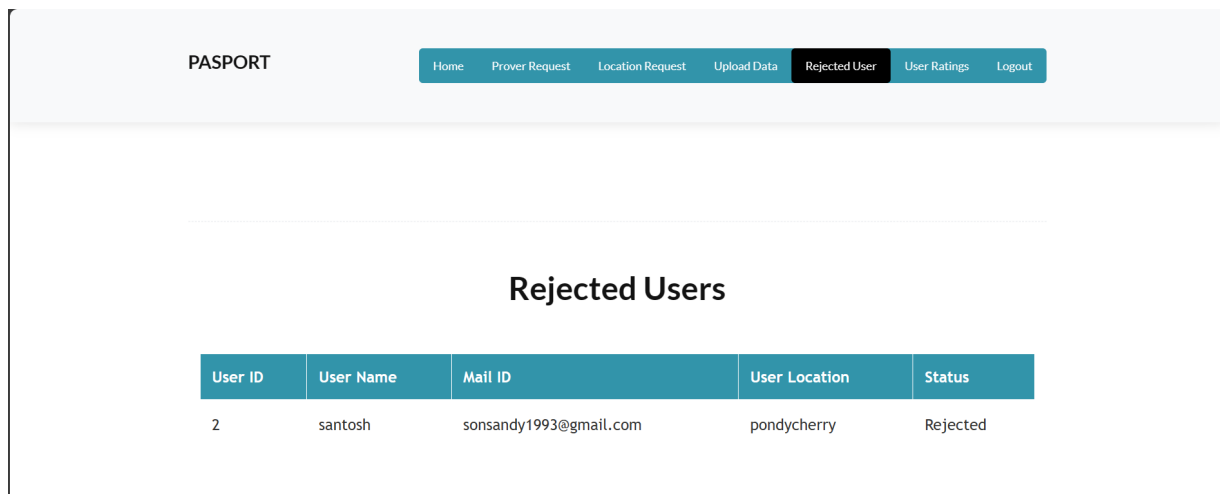


The screenshot displays the 'PASPORT' application interface. At the top, a navigation bar includes links for 'Home', 'Prover Request', 'Location Request', 'Upload Data' (which is the active tab), 'Rejected User', 'User Ratings', and 'Logout'. The main content area is divided into two sections. On the left, there is a vertical image of a person in a blue suit holding a glowing smartphone, with a background of digital icons. On the right, there is a form for uploading data. The form includes a 'Select Data Type' dropdown menu with options for 'Coffee', 'Food', 'Shopping', and 'Pizza'. Below this is a text input field labeled 'Enter Description'. Further down is a 'Location:' label followed by a text input field labeled 'Enter Location'. At the bottom, there is a 'Choose Image:' label followed by a file selection area with a 'Choose File' button and the text 'No file chosen'.

Fig:5.5 UPLOAD DATA

5.3.4 Rejected Users Module

This module maintains a log of users whose registration or location proof requests have been denied. It provides the verifier with a record of such incidents, including the reasons for rejection. Reasons may include discrepancies in the information provided, failure to meet the system's security criteria, or suspicion of fraudulent activity. This module is crucial for auditing purposes and for maintaining the security and integrity of the system.



The screenshot shows a web application interface for 'PASPORT'. At the top, there is a navigation bar with the following links: Home, Prover Request, Location Request, Upload Data, Rejected User (which is highlighted), User Ratings, and Logout. Below the navigation bar, the main heading 'Rejected Users' is centered. Underneath the heading is a table with the following data:

User ID	User Name	Mail ID	User Location	Status
2	santosh	sonsandy1993@gmail.com	pondycherry	Rejected

Fig:5.6 REJECTED USERS

5.3.5 User Ratings Module

Here, the verifier can monitor and review the ratings submitted by users for various products or services. This module is important for ensuring that the ratings reflect genuine user experiences and are based on verified location proofs. It helps maintain the credibility of the rating system and provides valuable feedback to service providers.

5.3.6 Logout Functionality

The logout feature is a security measure that allows the verifier to securely exit the console when their session is complete. This ensures that the console remains protected against unauthorized access and that all sensitive information within the system is safeguarded.

CHAPTER 6

RESULTS AND DISSCUSION

The following points outline the key findings and discussions based on the system's implementation and the experimental results obtained:

6.1 Verification of Genuine Location Claims

- The system successfully verified genuine location claims, allowing users to access location-based services. This verification process is critical in ensuring that only users who are physically present at a given location can access the service or resource, thereby preventing fraudulent activities.
- The implementation of the PASPORT scheme demonstrated that the integration of the P-TREAD protocol effectively reduced the success probability of Prover-Witness collusion attacks, which is a significant advancement over existing LP schemes.

6.2 User Access to Location-Based Services

- Upon successful location verification, users were granted access to the service, in this case, the ability to provide ratings for products. This feature highlights the practical application of the PASPORT project in real-world scenarios, such as online rating and review platforms where the authenticity of user reviews is paramount.
- The system's ability to authenticate user location claims ensures that the ratings given are based on actual user experiences, thereby enhancing the credibility of the rating system.

PASPORT

HomeLocation RequestWitness RequestLocation VerifySearchLogout

Search Product



Type :

Select Data Type

Location :

Enter Location

Search

Fig:6.1 USER ACCESSING LB SERVICES

PASPORT

HomeProver RequestLocation RequestUpload DataRejected UserUser RatingsLogout

User Ratings

Brand ID	User Name	User Location	Brand Name	Type	Brand Location	Rating
2	abdul	Pondy	Ciclo Cafe	Coffee	chennai	4
1	abdul	Pondy	Absolute Barbecue	Food	Pondicherry	4
1	abdul	Pondy	Absolute Barbecue	Food	Pondicherry	4

Fig:6.2 GENIUNE USER RATINGS

6.3 System Performance and Efficiency

- The prototype implementation on the Android platform showed that the PASPORT scheme operates faster than existing distributed LP schemes and requires lower computational resources. This efficiency is crucial for the widespread adoption of the system in various location-based applications.
- The system's decentralized architecture proved to be suitable for ad hoc scenarios, demonstrating that a fixed wireless infrastructure is not necessary for the generation and verification of LPs.

6.4 Privacy Preservation

- The PASPORT scheme successfully protected user privacy during the LP generation and verification process. Users were able to submit LP requests anonymously, and witnesses generated LPs without revealing their identities, which is a significant improvement in terms of privacy compared to other LP schemes.
- The privacy-aware distance bounding protocol, P-TREAD, ensured that the proximity checking process did not compromise user privacy, addressing one of the key challenges in location-based services.

6.5 Security and Reliability

- The system's architecture and protocols were designed to be resilient to various security threats, including Prover-Prover and Prover-Witness collusions. The experimental results confirmed the robustness of the PASPORT scheme in mitigating these threats.
- The verifier console played a crucial role in maintaining the integrity of the system by managing prover requests, location requests, and user ratings effectively. The console's modules for handling new user registrations, location proof requests, and data uploads contributed to the overall security and reliability of the system.

CHAPTER 7

CONCLUSION

7.1 CONCLUSION

In conclusion, the PASPORT project represents a significant advancement in the realm of location-based services, addressing the pressing challenge of location spoofing with a novel and robust framework. The project's innovative approach, characterized by its decentralized architecture and the integration of the P-TREAD protocol, has set a new benchmark for the integrity and privacy of location data. The PASPORT scheme has successfully demonstrated its ability to empower users to generate and verify location proofs in a manner that is both secure and respectful of their privacy. By enabling mobile users to act as witnesses for one another, the framework has effectively mitigated the risk of collusion attacks, ensuring that location proofs are unforgeable and non-transferable. This has been achieved without compromising the ease of use or the accessibility of the system for legitimate users. The introduction of P-TREAD, a privacy-aware distance bounding protocol, has further enhanced the system's security, making the proximity checking process private and resistant to prover-prover and prover-witness collusion attacks. The successful implementation of a prototype on the Android platform and the positive results from extensive experiments have validated the efficacy of the PASPORT scheme in protecting location-based applications against fraudulent submissions. As we look to the future, the PASPORT project holds the promise of transforming the landscape of location-based services. Its ability to provide a secure and private framework for location proof generation and verification is not just a technical achievement but also a step towards fostering greater trust among users and service providers. The project's contributions to the field of location-based services are expected to have a lasting impact, paving the way for more reliable, secure, and user-centric applications in the years to come.

7.2 Future Enhancements

- The discussions also touched upon potential future enhancements to the PASPORT framework, such as the introduction of location granularity features and the exploration of a blockchain-based incentive mechanism to further encourage user participation and cooperation in the LP generation process.

REFERENCES

- [1] 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.
- [2] G. Avoine et al., "Security of distance-bounding: A survey," *ACM Compute.Surv.*, vol. 51, no. 5, pp. 1–33, Jan. 2019.
- [3] 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-Market-2018-2023-Projected-Grow>.
- [4] J. Li, G. Liu, C. Yan, and C. Jiang, "LORI: A learning-to-rank-based integration method of location recommendation," *IEEE Trans. Compute. Social Syst.*, vol. 6,no. 3, pp. 430–440, Jun. 2019.
- [5] L. Zheng, G. Liu, C. Yan, and C. Jiang, "Transaction fraud detection based on total order relation and behavior diversity," *IEEE Trans. Compute.Social Syst.*,vol.5, no. 3, pp. 796–806, Sep. 2018.
- [6] 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.
- [7] Q. D. Vo and P. De, "A survey of fingerprint-based outdoor localization," *IEEE Common. Surveys Tuts.*, vol. 18, no. 1, pp. 491–506, 1st Quart., 2016.

- [8] 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.
- [9] S. Gambs, C. Onete, and J. M. Robert, "Prover anonymous and deniable distance bounding authentication," in *Proc. Asia CCS*, 2014, pp. 501–506.
- [10] S. Mauw, Z. Smith, J. Toro-Pozo, and R. Trujillo-Rasua, "Distance bounding protocols: Verification without time and location," in *Proc. IEEE Symp. Secure. Privacy (SP)*, San Francisco, CA, USA, May 2018, pp. 549–566.
- [11] S. Vaudenay, "Private and secure public-key distance bounding: Application to NFC payment," in *Proc. Financial Cryptor.*, in *Lecture Notes in Computer Science*. Berlin, Germany: Springer, 2015, pp. 207–216.
- [12] T. Chothia, J. D. Ruiter, and B. Smyth, "Modelling and analysis of a hierarchy of distance bounding attacks," in *Proc. 27th USENIX Secure. Symp. (USENIX Security)*, Apr. 2018.
- [13] 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.
- [14] Y. Zheng, M. Li, W. Lou, and Y. T. Hou, "Location based handshake and private proximity test with location tags," *IEEE Trans. Depend. Sec. Compute.*, vol. 14, no. 4 pp. 406–419, Jul./Aug. 2017.
- [15] 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.

APPENDIX

A. SOURCE CODE

Decryption.java

```
/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */
package PASPORT;

/**
 *
 * @author java1
 */
import com.sun.org.apache.xerces.internal.impl.dv.util.Base64;
import java.io.ByteArrayOutputStream;
import java.io.FileInputStream;
import java.io.FileWriter;
import java.util.Scanner;
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import javax.crypto.spec.SecretKeySpec;
import javax.swing.JOptionPane;
import sun.misc.BASE64Decoder;
import sun.misc.BASE64Encoder;

public class Decryption
{
    public String decrypt(String txt,String skey)
```

```

{
    String decryptedtext = null;
    try
    {
        //converting string to secretkey
        byte[] bs=Base64.decode(skey);
        SecretKey sec=new SecretKeySpec(bs, "AES");
        System.out.println("converted string to seretkey:"+sec);
        System.out.println("secret key:"+sec);
        Cipher aesCipher = Cipher.getInstance("AES");//getting AES instance
        aesCipher.init(Cipher.ENCRYPT_MODE,sec);//initiating ciper encryption using
        secretkey
        byte[] byteCipherText =new BASE64Decoder().decodeBuffer(txt); //encrypting
        data
        // System.out.println("ciper text:"+byteCipherText);

        aesCipher.init(Cipher.DECRYPT_MODE,sec,aesCipher.getParameters());//initiating
        ciper decryption
        byte[] byteDecryptedText = aesCipher.doFinal(byteCipherText);
        decryptedtext = new String(byteDecryptedText);
        System.out.println("Decrypted Text:"+decryptedtext);
    }
    catch(Exception e)
    {
        System.out.println(e);
    }
    return decryptedtext;
}
}
Encryption.java
/*

```

* To change this template, choose Tools | Templates

* and open the template in the editor.

*/

```
package PASPORT;
```

```
/**
```

```
 *
```

```
 * @author java1
```

```
 */
```

```
import javax.crypto.Cipher;
```

```
import javax.crypto.SecretKey;
```

```
import sun.misc.BASE64Encoder;
```

```
public class Encryption
```

```
{
```

```
public String encrypt(String text,SecretKey secretkey)
```

```
{
```

```
    String plainData=null,cipherText=null;
```

```
        try
```

```
        {
```

```
            plainData=text;
```

```
            Cipher aesCipher = Cipher.getInstance("AES");//getting AES instance
```

```
            aesCipher.init(Cipher.ENCRYPT_MODE,secretkey);//initiating cipher encryption  
using secretkey
```

```
            byte[] byteDataToEncrypt = plainData.getBytes();
```

```
            byte[] byteCipherText = aesCipher.doFinal(byteDataToEncrypt);//encrypting  
data
```

```
            // System.out.println("cipher text:"+byteCipherText);
```

```
            cipherText = new BASE64Encoder().encode(byteCipherText);//converting  
encrypted data to string
```

```
            System.out.println("\n Given text : "+plainData+" \n Cipher Data : "+cipherText);
```

```
        }
```

```
        catch(Exception e)
```

```

        {
            System.out.println(e);
        }
    }
    return cipherText;
}
}

```

TripleDES.java

```

package PASPORT;

/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */
/**
 *
 * @author jp
 */
import java.security.spec.KeySpec;
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.DESedeKeySpec;
import org.apache.commons.codec.binary.Base64;

public class TrippleDes {
    private static final String UNICODE_FORMAT = "UTF8";
    public static final String DESEDE_ENCRYPTION_SCHEME = "DESEde";
    private KeySpec ks;
    private SecretKeyFactory skf;
    private Cipher cipher;
    byte[] arrayBytes;

```

```

private String myEncryptionKey;
private String myEncryptionScheme;
SecretKey key;
public TrippleDes() throws Exception {
    myEncryptionKey = "ThisIsSpartaThisIsSparta";
    myEncryptionScheme = DESEDE_ENCRYPTION_SCHEME;
    arrayBytes = myEncryptionKey.getBytes(UNICODE_FORMAT);
    ks = new DESedeKeySpec(arrayBytes);
    skf = SecretKeyFactory.getInstance(myEncryptionScheme);
    cipher = Cipher.getInstance(myEncryptionScheme);
    key = skf.generateSecret(ks);
}
public String encrypt(String unencryptedString) {
    String encryptedString = null;
    try {
        cipher.init(Cipher.ENCRYPT_MODE, key);
        byte[] plainText = unencryptedString.getBytes(UNICODE_FORMAT);
        byte[] encryptedText = cipher.doFinal(plainText);
        encryptedString = new String(Base64.encodeBase64(encryptedText));
    } catch (Exception e) {
        e.printStackTrace();
    }
    return encryptedString;
}
public String decrypt(String encryptedString) {
    String decryptedText=null;
    try {
        cipher.init(Cipher.DECRYPT_MODE, key);
        byte[] encryptedText1 = encryptedString.getBytes(UNICODE_FORMAT);
        byte[] encryptedText = Base64.decodeBase64(encryptedText1);

```

```

        byte[] plainText = cipher.doFinal(encryptedText);
        decryptedText= new String(plainText);
    } catch (Exception e) {
        e.printStackTrace();
    }
    return decryptedText;
}

/* public static void main(String args []) throws Exception
{
    TrippleDes td= new TrippleDes();
    String target="imparator";
    String encrypted=td.encrypt(target);
    String decrypted=td.decrypt(encrypted);
    System.out.println("String To Encrypt: "+ target);
    System.out.println("Encrypted String:" + encrypted);
    System.out.println("Decrypted String:" + decrypted);
}
*/
}

```

Locationencryption.java

```

/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */
package PASPORT;
import com.oreilly.servlet.MultipartRequest;
import com.sun.org.apache.xerces.internal.impl.dv.util.Base64;
import DBconnection.SQLconnection;

```

```

import java.io.BufferedReader;
import java.io.File;
import java.io.FileReader;
import java.io.FileWriter;
import java.io.IOException;
import java.io.PrintWriter;
import java.security.SecureRandom;
import java.sql.Connection;
import java.sql.ResultSet;
import java.sql.Statement;
import java.text.DateFormat;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Random;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import javax.servlet.http.HttpSession;

/**
 *
 * @author java3
 */
public class Location_encryption extends HttpServlet {

    /**
     * Processes requests for both HTTP GET and
     * POST
     * methods.

```

```

*
* @param request servlet request
* @param response servlet response
* @throws ServletException if a servlet-specific error occurs
* @throws IOException if an I/O error occurs
*/
protected void processRequest(HttpServletRequest request, HttpServletResponse
response)
    throws ServletException, IOException {
    response.setContentType("text/html;charset=UTF-8");
    PrintWriter out = response.getWriter();
    try {

        String loc = request.getParameter("location");
        Connection con = SQLconnection.getconnection();
        KeyGenerator Attrib_key = KeyGenerator.getInstance("AES");
        Attrib_key.init(128);
        SecretKey secretKey = Attrib_key.generateKey();
        System.out.println("+++++++ key:" + secretKey);
        Encryption e = new Encryption();
        String en_location = e.encrypt(loc, secretKey);
        //storing encrypted file
        byte[] b = secretKey.getEncoded();
        String Dkey = Base64.encode(b);
        System.out.println("converted secretkey to string:" + Dkey);
        HttpSession session = request.getSession();
        HttpSession user = request.getSession(true);
        String pmail = user.getAttribute("umail").toString();
        String pname = user.getAttribute("uname").toString();
        String pid = user.getAttribute("uid").toString();

```

```

DateFormat dateFormat = new SimpleDateFormat("yyyy/MM/dd HH:mm:ss");
Date date = new Date();
String time = dateFormat.format(date);
System.out.println("current Date " + time);
Statement st = con.createStatement();
Statement st1 = con.createStatement();

System.out.println("Check-----
>>>>>");

ResultSet rs = st.executeQuery(" Select * from location where pid =" + pid + "
AND pname = " + pname + "");
if (rs.next()) {
    response.sendRedirect("location_request1.jsp?location_encrypted");

} else {
    ResultSet rs1 = st1.executeQuery(" Select * from user_reg where id =" +
pid + " AND name = " + pname + "");
    if (rs1.next()) {
        String org_location = rs1.getString("address");

        int i = st.executeUpdate("insert into location(pname, pmail, pid, location,
time, dkey, en_location, org_location)values(" + pname + "," + pmail + "," + pid + "," +
+ loc + "," + time + "," + Dkey + "," + en_location + "," + org_location + ")");
        if (i != 0) {
            response.sendRedirect("location_request1.jsp?location_encrypted");
        } else {
            System.out.println("Error in SQL Syntex");
        }
    } else {
        System.out.println("Error in SQL Syntex");
    }
}

} catch (Exception e) {

```

```

        out.println(e);
    } finally {
        out.close();
    }
}

```

// <editor-fold defaultstate="collapsed" desc="HttpServlet methods. Click on the + sign on the left to edit the code.">

```

/**
 * Handles the HTTP <code>GET</code> method.
 *
 * @param request servlet request
 * @param response servlet response
 * @throws ServletException if a servlet-specific error occurs
 * @throws IOException if an I/O error occurs
 */
@Override
protected void doGet(HttpServletRequest request, HttpServletResponse response)
    throws ServletException, IOException {
    processRequest(request, response);
}

/**
 * Handles the HTTP <code>POST</code> method.
 *
 * @param request servlet request
 * @param response servlet response
 * @throws ServletException if a servlet-specific error occurs
 * @throws IOException if an I/O error occurs
 */
@Override

```

```

    protected void doPost(HttpServletRequest request, HttpServletResponse
response)
        throws ServletException, IOException {
    processRequest(request, response);
}

/**
 * Returns a short description of the servlet.
 *
 * @return a String containing servlet description
 */
@Override
public String getServletInfo() {
    return "Short description";
} // </editor-fold>
}

```

PASPORT: A SECURE AND PRIVATE LOCATION PROOF GENERATION

Sathwik ¹, BINDU NAIDU ², L. Sujihelen ³
Sathyabama Institute of Science and Technology, Chennai
sujihelen@gmail.com

Abstract—Recently, there has been a fast growth in vicinity primarily based systems and applications in which users publish their place facts to carrier providers if you want to gain get entry to to a provider, resource, or reward. We have visible that during these programs, dishonest users have an incentive to cheat on their region. Unfortunately, no effective safety mechanism has been followed via carrier providers against these faux vicinity submissions. This is a critical trouble that reasons extreme results for these packages. Motivated by using this, we advise the Privacy-Aware and Secure Proof Of Privacy (PASPORT) scheme in this text to address the trouble. Using PASPORT, users publish a region evidence (LP) to carrier providers to prove that their submitted vicinity is true PASPORT has a decentralized architecture designed for advert hoc situations wherein mobile customers can act as witnesses and generate LPs for each other. It gives user privacy protection in addition to safety houses, such as unforgeability and non-transferability of LPs. Furthermore, the PASPORT scheme is resilient to prover–prover collusions and extensively reduces the success probability of prover–witness collusion assaults. To in addition make the proximity checking process private, we advise P-TREAD, a privateness-conscious distance bounding protocol and combine it into PASPORT. To validate our model, we enforce a prototype of the proposed scheme on the Android

platform. Extensive experiments suggest that the proposed method can successfully protect vicinity-primarily based applications against fake submissions.

INTRODUCTION

What is Secure Computing?

Computer security (Also called cyber protection or IT Security) is data security as implemented to computers and networks. The discipline covers all of the procedures and mechanisms by which computer-primarily based equipment, records and services are blanketed from unintended or unauthorized get entry to, exchange or destruction. Computer security additionally includes protection from unplanned activities and herbal failures. Otherwise, in the laptop enterprise, the time period safety – or the word laptop security – refers to strategies for making sure that information saved in a laptop can't be read or compromised through any people without authorization. Most pc security features contain statistics encryption and passwords. Data encryption is the interpretation of data right into a form that is unintelligible with out a deciphering mechanism. A password is a secret phrase or phrase that gives a consumer get admission to to a specific program or system. Diagram really explain the about the at ease computing

Working conditions and basic needs in the secure computing:

If you do not take fundamental steps to defend your work pc, you placed it and all of the records on it at hazard. You can potentially compromise the operation of other computers to your business enterprise's network, or even the functioning of the community as a whole.

Physical security:

Technical measures like login passwords, anti-virus are crucial. (More about the ones below) However, a comfortable physical area is the first and extra essential line of defense.

Is the vicinity you preserve your workplace pc at ease enough to prevent robbery or get right of entry to to it at the same time as you are away? While the Security Department presents insurance throughout the Medical Center, it only takes seconds to scouse borrow a laptop, in particular a portable tool like a laptop or a PDA. A pc ought to be secured like any other treasured possession while you are not gift.

Human threats aren't the handiest concern. Computers can be compromised by means of environmental mishaps (e.G., water, espresso) or physical trauma. Make sure the physical vicinity of your computer takes account of these risks as well.

Access passwords:

The University's networks and shared records structures are protected in component by means of login credentials (user-IDs and passwords). Access passwords are also an critical protection for non-public computer systems in most circumstances. Offices are typically open and shared spaces, so bodily access to computers can't be absolutely managed.

To defend your computer, you must take into account putting passwords for especially touchy applications residing at the computer (e.G., records analysis software), if the software program affords that capability.

Prying eye protection:

Because we deal with all sides of scientific, research, educational and administrative statistics here on the medical campus, it's miles essential to do the entirety possible to decrease publicity of information to unauthorized individuals.

Anti-virus software:

Up-to-date, well configured anti-virus software is crucial. While we've got server-aspect anti-virus software program on our network computers, you still need it at the patron side (your pc).

Firewalls:

Anti-virus merchandise inspect files on your laptop and in email. Firewall software program and hardware screen communications between your computer and the outdoor international. That is essential for any networked computer.

Software updates:

It is essential to keep software up to date, mainly the operating gadget, anti-virus and anti-adware, e mail and browser software program. The most recent variations will include fixes for observed vulnerabilities. Almost all anti-virus have automatic update capabilities (such as SAV). Keeping the "signatures" (virtual patterns) of malicious software

program detectors up to date is essential for those merchandise to be powerful.

1. Keep secure backups:

Even if you take these kinds of safety steps, awful matters can still show up. Be prepared for the worst by making backup copies of crucial data, and retaining the ones backup copies in a separate, comfy vicinity. For example, use supplemental hard drives, CDs/DVDs, or flash drives to shop essential, tough-to-replace information.

2. Report problems:

If you agree with that your pc or any facts on it has been compromised, you have to make an data security incident report. That is required by University coverage for all facts on our structures, and legally required for fitness, education, monetary and every other type of file containing identifiable non-public data.

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.

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.

LITERATURE SURVEY

1) Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges, and countermeasures

Authors: p. asuquo et al

Location-primarily based offerings (LBSSs) have won reputation due to the advances in mobile and communicate technology. LBS provide customers with relevant statistics primarily based on their region. In

spite of the appropriate functions provided by LBS, the geographic locations of users are not accurately covered. Location privateness is one of the primary demanding situations in vehicular and cell networks. In this paper, we analyze the safety and privacy necessities for LBS in vehicular and cell networks. Specifically, this paper covers privateness improving technology and cryptographic methods that offer place privacy in vehicular and cell networks. The exclusive methods proposed in the literature are compared and open studies regions are diagnosed.

2) A survey of fingerprint-based outdoor localization

Authors: q. d. vo and p. de

Location-based services (LBSs) have received reputation because of the advances in mobile and communicate technologies. LBS offer customers with applicable information based totally on their area. In spite of the desirable functions provided by way of LBS, the geographic places of users aren't thoroughly included. Location privacy is one of the important demanding situations in vehicular and mobile networks. In this paper, we analyze the security and private ness requirements for LBS in vehicular and cellular networks. Specifically, this paper covers private ness enhancing technology and cryptographic techniques that provide location private ness in vehicular and mobile networks. The extraordinary strategies proposed in the literature are compared and open research regions are recognized.

3) An exploration to location-based service and its privacy preserving techniques: A survey

Authors: R. Gupta and U. P. Rao

Mobile devices today are swaggering computing capability and memory at par or at times even better to that observed in computer private computers. A wireless interconnection has turned out to be appreciably extra quite simply on hand in recent times. As individuals are developing mobile with reference

to the quick life-style and working sample, a new, smarter machine got here into lifestyles that is termed as 'Location Based Service' (LBS). Such a system amalgamates the region records of a person with clever programs to deliver demanded services. Although LBS offers most important openings for a massive type of markets and outstanding comfort to the end person, it also affords a subtle privateness assault to the person's vicinity records. Threat to the privateness sneaks into the device because of the prerequisite of sending consumer's contemporary vicinity to the LBS issuer to achieve associated services. Since the extent of information gathered from dynamic or stationary cellular users the usage of LBS can be excessive, it's far crucial to outline the frameworks and structures in a manner this is secure and maintain the location facts private. In this paper, we perform an exploratory survey about the numerous techniques which have been suggested via many researchers based on centralized and allotted methods, to preserve the area privacy of the user. A huge component of these strategies has a trade-off between privateness, efficiency, applicability and satisfactory of service. This paper info and analyzes the various present strategies for maintaining location privacy of the collaborating user in LBS.

4) Location based handshake and private proximity test with location tags

Authors: Y. Zheng, M. Li, W. Lou, and Y. T. Hou

A place proximity take a look at carrier lets in cell users to determine whether they may be in near proximity to each different, and has observed severa programs in mobile social networks. Unfortunately, existing answers generally display an awful lot of customers' personal vicinity information during a proximity take a look at. They also are vulnerable to area dishonest wherein an attacker reviews false places

to gain a bonus. Moreover, the preliminary accept as true with establishment among unexpected customers in huge scale cellular social networks has been a hard challenge. In this paper, we recommend a unique scheme that permits a user to carry out (1) a location based handshake that establishes at ease communications among strangers, who do no longer have a pre-shared mystery, and (2) a privateness-retaining proximity take a look at with out revealing the consumer's real region to the server or other customers not inside the proximity. The proposed scheme is based totally on a novel concept, i.E., spatial-temporal location tags, and we recommend a location tag creation technique using environmental indicators that gives an unforgeable location evidence. We use Bloom filters to successfully represent customers' place tags and community regions. We exploit fuzzy extractor, a light-weight cryptographic primitive, to extract shared secrets and techniques among matching area tags. We conduct widespread analysis, simulation, and real experiments to demonstrate the feasibility, safety, and performance of our scheme.

5) Privacy-preserving location proof for securing large-scale database-driven cognitive radio networks

Authors: Y. Li, L. Zhou, H. Zhu, and L. Sun

The latest Federal Communications Commission (FCC) ruling has enforced database-driven cognitive radio networks (CRNs), wherein all secondary customers (SUs) can query a database to acquire spectrum availability information (SAI). Database-driven CRNs are appeared as a promising approach for dynamic and relatively green spectrum management paradigm for large-scale Internet of Things (IoT). However, as a standard area-based carrier (LBS), before imparting services to the user, there is no verification of the queried region, which may be very liable to a place spoofing attack. A malicious user can record a fake vicinity to the database and access the

channels that won't be to be had for its place. This will introduce serious interference to the primary customers (PUs). In this study, we pick out a new form of attack coined as area cheating assault, which allows an attacker to spoof other users to every other location and make them question the database with wrong vicinity, or lets in a malicious user to forge area arbitrarily and query the database for services. To thwart this assault, we suggest a novel infrastructure-based totally approach that relies on the existing WiFi or cellular network get entry to points (or AP) to offer privacy-preserving region proof. With the proposed answer, the database can verify the places with out understanding the person's accurate place. We perform complete experiments to assess the overall performance of the proposed method. Experimental outcomes show that our method, except supplying region proofs efficiently, can substantially enhance the person's location privacy.

SYSTEM REQUIREMENTS:

Hardware requirements:

System : Pentium i3 Processor
 Hard Disk : 500 GB.
 Monitor : 15'' LED
 Input Devices : Keyboard, Mouse
 Ram : 2 GB

Software requirements:

Operating system : Windows 10.
 Coding Language : JAVA.
 Tool : Net beans 8.2
 Database : MYSQL

EXISTING SYSTEM:

Saroiu and Wolman proposed a way in which the AP pronounces beacon frames consisted of a sequence number. To reap an LP, customers ought to signal the final transmitted collection number with their non-public key and send it again to the AP along side their public key (the access factor proclaims beacons each 100 ms). This makes the gadget resistant against

terrorist frauds since the malicious prover does now not have enough time to acquire the series wide variety from the adversary and signal and send it again to the adversary. However, the proposed set of rules has privateness problems due to the fact users need to monitor their identity publicly.

□ APPLAUSE delivered via Zhu and Cao is one of the pioneer studies works on disbursed LP systems. In APPLAUSE, cellular devices use their quick range Bluetooth interface to talk with their nearby devices who request an LP. To maintain users' vicinity privacy, they want to select a hard and fast of M pseudonyms and trade them periodically. These pseudonyms are taken into consideration as customers' public keys, which are required to be registered with a relied on certificates authority (CA) at the side of the associated private keys. However, changing pseudonyms regularly creates a high level of computation and communicate overhead.

Disadvantages

To the great of our knowledge, we discovered that each one the modern-day LP schemes be afflicted by at least one key downside.

□ First, a number of those schemes are prone to prover-prover (P-P) collusion. In this attack, a far off malicious prover colludes with a unethical user (positioned at a preferred website online) to attain an LP. The cheating consumer submits an LP request to the neighbor witness devices on behalf of the faraway prover. This protection chance is referred to as terrorist fraud inside the literature.

□ Second, not one of the cutting-edge allotted schemes provide a reliable answer for Prover–Witness (P–W) collusions. In this attack, a dishonest consumer

acts as a witness for a faraway malicious prover and generates a faux LP for him.

□ Finally, in some schemes, vicinity privateness has not been taken into consideration, i.E., users broadcast their identity for neighbor gadgets or a third party server all through the LP generation or submission method.

PROPOSED_SYSTEM:

To the exceptional of our information, we discovered that each one the current LP schemes be afflicted by as a minimum one key drawback.

□ First, some of those schemes are susceptible to prover-prover (P-P) collusion. In this assault, a remote malicious prover colludes with a unethical person (located at a favored site) to gain an LP. The cheating consumer submits an LP request to the neighbor witness devices on behalf of the far flung prover. This protection chance is called terrorist fraud in the literature.

□ Second, not one of the cutting-edge disbursed schemes offer a dependable solution for Prover–Witness (P–W) collusions. In this attack, a unethical user acts as a witness for a remote malicious prover and generates a fake LP for him.

□ Finally, in some schemes, area privateness has no longer been taken into consideration, i.E., customers broadcast their identity for neighbor devices or a 3rd birthday party server in the course of the LP technology or submission manner.

Advantages

Our experimental outcomes show that the proposed scheme works quicker than the prevailing allotted LP schemes and requires low computational sources.

We propose a personal model of TREAD, i.e., PTREAD, through which a prover device can anonymously broadcast its LP request for neighbor witnesses, at the same time as he/she blessings from the TREAD safety guarantees.

PASPORT is proof against prover-prover collusions and reduces the fulfillment possibility of prover-witness collusions to a negligible price.

It isn't always feasible for a malicious prover to create an LP himself without proving his area to a qualified witness.

PASSPORT is proof against mafia frauds.

GOALS:

The number one dreams inside the layout of the UML are as follows:

1. Provide users with a geared up-to-use, expressive visual modeling language which will broaden and change meaningful fashions.
2. Provide extensibility and specialization mechanisms to extend the center principles.
3. Be impartial of unique programming languages and improvement approaches.
4. Provide a formal basis for expertise the modeling language.
5. Encourage the increase of OO equipment market.
6. Support better stage development principles which includes collaborations, frameworks, styles and components.
7. Integrate first-rate practices.

MODULES:

- *Architecture and Entities*
- *Trust and Thread Model*
- *Test*
- *Witness*

- *Verify*

Modules description:

Architecture and Entities:

The proposed device structure is the gadget has a allotted architecture and includes 3 kinds of entities, i.e., prover, witness, and verifier. A prover is a cellular consumer who calls for to prove his/her vicinity to a verifier. A witness is the entity that accepts to difficulty an LP for a neighboring prover upon request. We assume that service vendors create enough incentives for mobile users to come to be a witness and certify other users' region. In PASPORT, we keep in mind witnesses as cell users. Finally, a verifier is the unit this is legal through the service issuer to verify LPs claimed by using provers. We count on that provers communicate with witnesses through a short-variety communicate interface, such as Wi-Fi or Bluetooth. This brief range conversation channel is meant to be nameless such that users can broadcast their messages over it without revealing their figuring out information, consisting of IP or MACcope

Trust and Thread Model:

We expect that cell users are registered with the carrier provider. Each person has a completely unique public-private pair key saved on his/her cellular device and authorized with the aid of a CA. Users' identification is decided via their public key, and we assume that users by no means share their non-public key with other users because they do no longer give their cell gadgets to others. Thus, in a collusion state of affairs, we suppose a malicious prover never goes that far to provide some other birthday party with his/her private key. We additionally expect that each one the messages exchanged between the entities might be eavesdropped by way of passive eavesdroppers. In the

subsequent, we speak the trust and threat model for each entity for my part

Prover:

It is assumed that the prover makes an attempt to obtain fake LPs. This may be executed via specific scenarios wherein a prover might try to provide the witnesses with fake data about his/her region to persuade them to generate LPs for him/her, manipulate the LP issued for him/her to change its vicinity or time discipline, try and thief an LP issued for any other user and use it for him/herself, and collude with different customers (provers or witnesses) to acquire LPs. Moreover, we expect that provers try and acquire the identification of witnesses.

Witness:

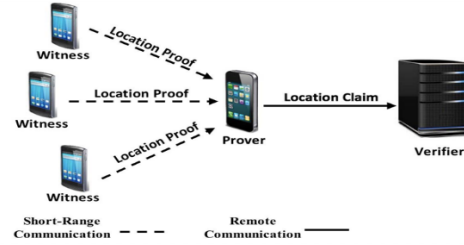
A witness may collude with a prover to generate a faux LP for him/her. In addition, a witness may also try to deny an LP that has been issued by using himself/herself. Witnesses are assumed to be curious about the provers' identification.

Verifier:

We assume that the verifier is trusted and by no means leaks users' identity and their spatiotemporal records. It is believed that the verifier keeps a regularly up to date list of

witnesses who are present at the given area and feature general to generate LPs for different users. The verifier accepts the LPs issued by these witnesses best. We suppose that provider companies create the important incentives to encourage egocentric users to collaborate with the machine. Otherwise, they won't generate LPs to shop their battery energy or lessen their communicate costs.

SYSTEM ARCHITECTURE:



RESULT AND DISSCUSSION

We have visible that in L.B.S packages, dishonest users have an incentive to cheat on their location. Unfortunately, no effective safety mechanism has been adopted by means of service companies against these fake region submissions. This is a important problem that causes severe results for these programs. LBSPs are prone to vicinity spoofing attacks due to the fact that cheating customers are incentivized to lie approximately their region and put up faux function records. In the modern online score and evaluation packages, customers' actual place isn't always demonstrated, which enables them to publish fake effective or poor opinions for his or her personal enterprise or their opponents.

Furthermore, in CRNs, malicious users can publish fake locations to the database to get admission to channels that aren't to be had of their area. In region-primarily based get entry to manage programs, attackers can advantage unauthorized get entry to to a system or resource via submitting fake vicinity claims. In interest-monitoring programs, coverage corporations may provide health insurance plans in which customers are presented discounts if they have a minimum degree of bodily interest

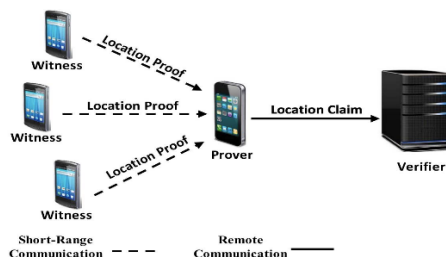
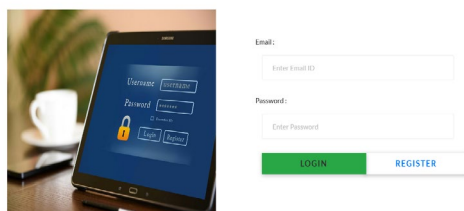
FUTURE ENHANCED

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.

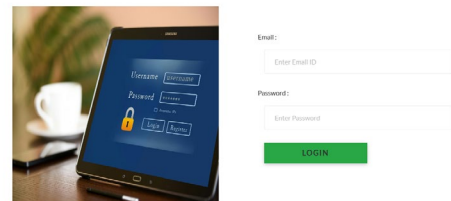
SCREEN SHOTS



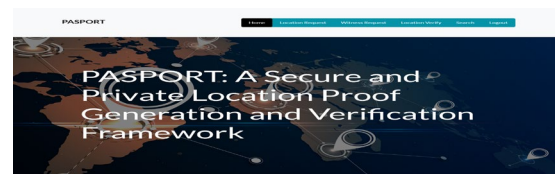
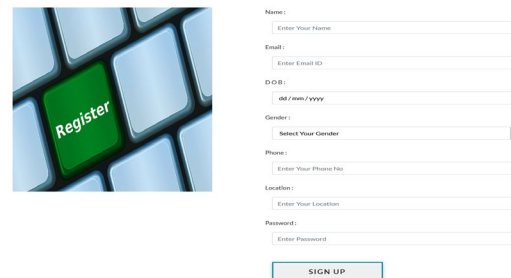
User Login



Verifier Login



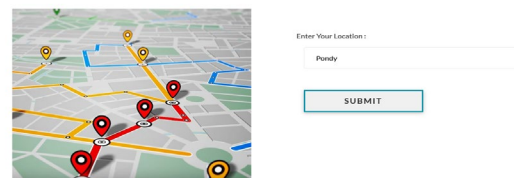
User Register



Welcome ABDUL



Encrypt Location



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-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.

[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.