An Efficient Privacy Preserving Location Proofs for Mobile users

Amrutha Bindu J N
Dept. of CSE
GSSSIETW Mysuru

Amrutha P
Dept. of CSE
GSSSIETW Mysuru

Arshitha P R
Dept. of CSE
GSSSIETW Mysuru

Chandana D
Dept. of CSE
GSSSIETW Mysuru

Usha Rani J
Assistant Professor
Dept. of CSE
GSSSIETW Mysuru

***Abstract*—Location-based services are rapidly becoming veryy popular nowadays. In addition to services based on users current location, many potential services depend on users location information, or their spatial-temporal origin. Intruders may lie about their spatial-temporal provenance without designing an appropriate security system for users to prove their past locations. In this paper our prototype implementation in the network domain is to prove users location with proof using CA [Certificate Authority] for encryption and decryption, for an organization. The encryption and decryption is doneusing SHA-1[Secured Hash Algorithm]. The SHA-1 algorithm is an efficient algorithm for encryption and decryption**

Keywords—Spatial-temporal provenance, Intruder, Certificate Authority, Secured Hash Algorithm

I. INTRODUCTION

As location-enabled mobile devices multiply in number, location- based services are rapidly becoming popular. Most of the current location- based services for mobile devices are based on user's present location, users discover their locations and share them with a server, then server performs appropriate action based on the location information and returns data/services to the users. In addition to user's present locations, there is an increased trend and motive to prove mobile user's respective geographical locations. As our prototype implementation in the network domain is to prove users location with proof using CA [Certificate Authority] for encryption and decryption, for an organization, is through an URL , it is necessary to use GPS for communication. GPS is a global navigation satellite system that provides geolocation and time information to the GPS receiver anywhere on or near the earth.

Today's location-based services uniquely rely on users' devices to determine their location, e.g., using GPS. However, it allows intruder users to fake his/her STP information. Therefore, there is a need to involve third parties in the creation of STP proofs in order to avoid frauds. Therefore, this opens a number of security and privacy issues. Location information is highly secret personal data. By knowing where a person was at a particular time, one can deduce his/her personal activities, political views, health status, and volunteer advertising, physical attacks or harassment. Therefore, mechanisms to preserve user's privacy and anonymity are important in an STP proof system. The communication takes place between three actors, a server and a CA which is used for encryption and decryption only. The three actors are a prover [Employee 1], a verifier [Admin] and a witness [Employee 2].

1.All the users have register with all their personal details, afer the registration the users gets acknowledgement from the server
2.After registration the user logs in to the server and requests for the private from the CA for encryption of the location details .
3.The encrypted data is send to the verifier, then the verifier selects the witness and requests the location proof from the witness.
4.The selected witness sends the encrypted location proof to the verifier for the verification.
5.The verifier then decrypts both location proofs from the user and witness and verifies the location proofs and sends the acknowledgement to the user.

II. RELATED WORK

W. Luo and U. Hengartner, "VeriPlace: A privacy-aware location proof architecture," in *Proc. ACM GIS*, 2010, pp. 23–32. A user's location is a crucial factor for enabling these services. Many services rely on users to correctly report their location. However, if there is an incentive, users might lie about their location. A location proof architecture enables users to collect proofs for being at a location and services to validate these proofs[2]. B. Waters and E. Felten, "Secure, private proofs of location," Department of Computer Science, Princeton University, Princeton, NJ, USA, Tech. Rep., 2003 –This paper present the design of a system that can securely prove the location of a mobile device. In the system the device attempts to prove its location to a party known as verifier using a local network[4].Fizza Abbas, Rasheed Hussain, "Privacy Preserving Cloud-Based Computing platform for using Location Based Services" , 2012- Integrate the mobile devices with cloud computing and name them as mobile cloud computing. To overcome the problems of mobile devices regarding storage, bandwidth, and battery life time due to their limited hardware specifications[5]. Ken Mano, Kazuhoro Minami, Hitoshi Maruyama, "Privacy-Preserving Publishing of Pseudonym-based Trajectory LocationData Set" ,2014 – To keep track of people's movement over a wide area by collecting GPS data from the mobile devices. Anomization is a common technique for publishing a location data set a in privacy preserving way, such a anomized data setlacks trajectory information of users[12].Farzana , " Preserving User Privacy in Pervasive Environments with a collaborative Model," , pp.84-93, 2013- this paper is based on privacy preferences according to place.Location findings are useful for designing privacy policy and user interfaces for pervasive computing[13].Wormhole attacks in wireless networks." In this paper, we introduce the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems[10]."Location privacy in urban sensing networks: research challenges and directions [security and privacy in emerging wireless networks]." as people are directly involved in the collection process, they often inadvertently reveal information about themselves, raising new and important privacy concerns. While standard privacy enhancing technologies exist,they do not fully cover the many peculiarities of these new pervasive applications. The ubiquitous nature of the communication and the storage of location traces compose a complex set of threats on privacy, which has been overviewed in this article. The latest advances in security and privacy protection strategies have been taken from this paper and we discuss how they fit with this new paradigm of people-centric sensing applications[11]. "Distance-bounding proof of knowledge to avoid real-time attacks". Traditional authentication is based on proving a knowledge of a private key corresponding to a given public key. In some situations, especially in the context of pervasive computing, it is additionally required to verify the physical proximity of the authenticated party in order to avoid a set of real time attacks. This protocol is used to prevent frauds where an intruder sits between a legitimate prover and a verifier and succeeds to perform the distance bounding process[6].

III PROPOSED WORK

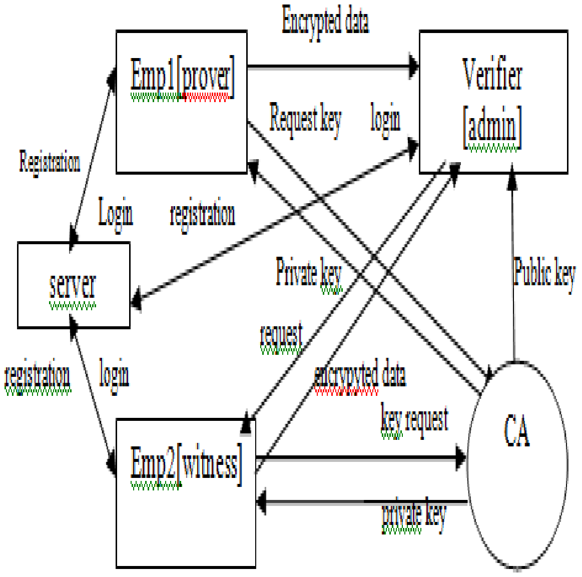

figure: Architecture of an efficient privacy preserving location proof for mobile users

Prover: A prover is a mobile device which tries to obtain STP proofs at a certain location.

- Witness: A witness is a device which is in proximity with the prover and is willing to create an STP proof for the prover upon receiving his/her request. The witness can be untrusted or trusted, and the trusted witness can be mobile or stationary (wireless APs). Collocated mobile users are untrusted.
- Verifier: A verifier is the party that the prover wants to show one or more STP proofs to and claim his/her presence at a location at a particular time.
- Certificate Authority (CA): The CA is responsible for managing cryptographic credentials for the other parties.

CA is also responsible for proof verification and trust evaluation.

The communication takes place between three actors, a server and a CA which is used for encryption and decryption only. The three actors are a prover [Employee 1], a verifier [Admin] and a witness [Employee 2].

The contributions of our paper can be summarized as:

1.All the users have register with all their personal details, afer the registration the users gets acknowledgement from the server
2.After registration the user logs in to the server and requests for the private from the CA for encryption of the location details .
3.The encrypted data is send to the verifier, then the verifier selects the witness and requests the location proof from the witness.
4.The selected witness sends the encrypted location proof to the verifier for the verification.
5.The verifier then decrypts both location proofs from the user and witness and verifies the location proofs
and sends the acknowledgement to the user.

IV IMPLEMENTATION DETAILS

The proposed protocol is implemented using SHA-1 algorithm. The SHA-1 is the widely used of the existing SHA hash functions and is employed in several widely used security applications and protocols. The tools used are eclipse with spring and php, postgresql 9.6, apache Tomcat and wampserver.

V RESULTS DISCUSSION

This protocol uses SHA-1 algorithm which ensures secured communication between a honest prover and a honest verifier. The employee in an organization can prove his location without any fraud. The fraud is prevented by encrypting and then decrypting the location proofs.

VI CONCLUSION AND FURTHER ENHANCEMENT

In our project, the protocol deals with the honest communication between a prover and a verifier. The employee can prove his location using Certificate.
Authority through verifier.The verifier cannot fraud the location proofs of prover and the witness because of encryption done by the prover and verifier.Hence no frauds can be done.
In future we can have a mobile application for it, where it can be implemented in actual organizations and see the results.

REFERENCES

[1] Wang, Xinlei, et al. "STAMP: enabling privacy- preserving location proofs for mobile users." IEEE/AC Transactions on Networking 24.6 (2016): 3276-3289.

[2] Luo, Wanying, and Urs Hengartner. "Veriplace: a privacy-aware location proof architecture." Proceeding of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems.ACM,2010..

[3] Zhu, Zhichao, and Guohong Cao. "Applaus: A privacy-preserving location proof updating system for location-based services." INFOCOM, 2011 Proceedings IEEE. IEEE, 2011.

[4] Waters, B., and E. Felten. Secure, private proofs of location. Princeton Computer Science. TR-667-03, 2003.

[5] Abbas, Fizza, et al. "Privacy preserving cloud- based computing platform (PPCCP) for using location based services." Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing. IEEE Computer Society, 2013.

[6] Bussard, Laurent, and Walid Bagga. "Distance- bounding proof of knowledge to avoid real-time attacks." Security and Privacy in the Age of Ubiquitous Computing (2005): 223-238.

[7] Reid, Jason, et al. "Detecting relay attacks with timing-based protocols." Proceedings of the 2nd ACM symposium on Information, computer and communications security. ACM, 2007.

[8] Afyouni, Imad, Ray Cyril, and Claramunt Christophe. "Spatial models for context-aware indoor navigation systems: A survey." Journal of Spatial Information Science 1.4 (2012): 85-123.

[9] Singelee, Dave, and Bart Preneel. "Location verification using secure distance bounding protocols." Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on. IEEE, 2005.

[10] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Wormhole attacks in wireless networks." IEEE journal on selected areas in communications 24.2 (2006): 370-380.

[11] Krontiris, Ioannis, Felix C. Freiling, and Tassos Dimitriou. "Location privacy in urban sensing networks research challenges and directions [security and privacy in emerging wireless networks]." IEEE Wireless Communications 17.5 (2010).

[12] Mano, Ken, Kazuhiro Minami, and Hiroshi Maruyama. "Privacy-preserving Publishing of Pseudonym- based Trajectory Location Data Set." Availability, Reliability and Security (ARES), 2013 Eighth International Conference on. IEEE, 2013.

[13] Rahman, Farzana, et al. "Preserving User Privacy in Pervasive Environments with a Collaborative Model." Software Security and Reliability-Companion (SERE-C), 2013 IEEE 7th International Conference on. IEEE, 2013.