ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Hierarchy Attribute Based Encryption Level of Location Proof for Mobile

Revathy .S[1], Hemalatha .T[2]
PG Student[1], Assistant Professor[2]
Department of Computer Science & Engineering
Krishnasamy College of Engineering & Technology, Cuddalore, Tamil Nadu, India

Abstract:
Location-based services can be implemented easily with increase of Smartphone users since 2008. Smartphone's are in-build with Global Positioning System device; with help of it much application has developed and reached its popularity. In addition to services based on user's current location, many potential services rely on user's location history. User location tracking and storing in database are highly confidential data if a user's location detail is shared to un-trusted user it may lead to heavy problem like user life risk issues. First developing a location based services suppose ifa store wants to offer discounts to frequent customers. Customers must be able to show evidence of their repeated visits in the past to the store.The above applications require users to be able to obtain proofs from the locations they visit. Hierarchy Attribute based Encryption is used to get the location details and location details are shared to the trusted user securely.

Key terms: Global Positioning System, Hierarchy Attribute based Encryption, location sharing.

I. INTRODUCTION

LOCATION-ENABLED mobile devices proliferate, location based services are rapidly becoming immensely popular. Most of the current location-based services for mobile devices are based on user's current location. User's locations are discovered and are shared with the server. In turn, the server performs computation based on the location information and returns data/services to the users. In addition to user's current locations, there is an increased trend and incentive to prove/validate mobile user's past geographical locations [1]. This opens a wide variety of new location-proof based mobile applications. Let us consider three examples: (1) A store wants to offer discounts to frequent customers. Customers must be able to show evidence of their repeated visits in the past to the store. (2) A company which promotes green commuting and wellness may reward their employees who walk or bike to work. The company may encourage daily walking goals of some fixed number of miles. Employees need to prove their past commuting paths to the company along with time history. This helps the company in reducing the healthcare insurance rates and move towards sustainable lifestyle. (3) On the battlefield, when a scout group is sent out to execute a mission, the commanding center may want every soldier to keep a copy of their location traces for investigation purpose after the mission. The above applications require users to be able to obtain proofs from the locations they visit. Users may then choose to present one or more of their proofs to a third-party verifier to claim their presence at a location at a particular time. In this paper, we define the past locations of a mobile user at a sequence of time points as the spatial-temporal provenance (STP) of the user, and a digital proof of user's presence at a location at a particular time as an STP proof [2]. Today's location-based services solely rely on user's devices to determine their location, e.g., using GPS [3]. However, it allows malicious users to fake their STP information. Therefore, we need to involve third parties in the creation of STP proofs in order to achieve the integrity of the STP proofs.

In this paper we propose an STP proof scheme named Spatial-Temporal provenance Assurance with Mutual Proofs (Data requester and admin should accept the request and send it to user approval). We have secure use HAE with two admin to make the location proof mechanism secure so that data requester gets proof of data are correct and user trust admin that their location details not shared without their permission [4][5].

II. BACKGROUND AND RELATED WORK

The notion of unforgeable location proofs was discussed by Waters [10].They proposed a secure scheme which device can use to get a location proof from a location manager. However, it requires users to know the verifiers as a prior. Saroiu [1] proposed a secure location proof mechanism; where users and wireless APs exchange their signed public keysto create timestamped location proofs. These schemes are susceptible to collusion attacks where users and wireless APs may collude to create fake proofs. VeriPlace [2] is a location proof architecture which is designed with privacy protection and collusion resilience. However, it requires three different trusted entities to provide security and privacy protection: a TTPL (Trusted Third Party for managing Location in formation), a TTPU (Trusted Third Party for managing User information) and a CDA (Cheating Detection Authority). Each trusted entity knows either a user's identity or his/her location, but not both. VeriPlace's collusion detection works only if users request their location proofs very frequently so that the long distance between two location proofs that are chronologically close can be considered as anomalies. This is not a realistic assumption because users should have the control over the frequency of their requests. [5] Proposed a scheme which relies on both location proofs from wireless APs and witness endorsements from Bluetooth-enabled mobile peers, so that no users can forge proofs without colluding with both wireless APs and other mobile peers at the same time. It eliminates the necessity of multiple trusted parties. Two privacy preserving schemes based on hash chains and Bloom filters respectively are

described for protecting the integrity of the chronological order of location proofs. All the above systems are centralized, that is, they all require central infrastructures (wireless APs) to act as the location authorities and generate location proofs. However, we want to design a framework that can also work for distributed scenario where users are far from any trusted AP.

III. HIERARCHY ATTRIBUTE BASED ENCRYPTION

Data requester can request for user location on particular period of time. Either can request for particular users in their location or user details in their location on particular time. Once request is passed by admin I and if user accepts the request admin II will share the location details to the user. User details will share by admin II only after the process completed. Data will be encrypted and shared to data requester.

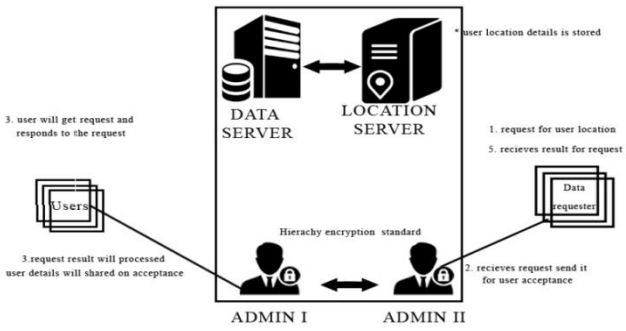

Figure.1.Architecture diagram for location proof for mobile users.

Admin I will get the request from data requester either based user details or location details on requested is validated it will be passed to user acceptance state. Admin II can view user acceptance status. Admin II will pass the user details based on the request to the data requester for their usage. Hierarchy attribute based encryption is used for data encryption to make sure that user location is not shared to any one with admin acceptance. User location will be monitored via GPS using a mobile app user location will be stored in the location server. Based on the user location & data requester location request user will get details about the data requester and the purpose of request then user can either can accept or reject. If users accept the request user details will be shared to data requester.

Hierarchical attribute--based encryption (HABE) by extending ciphertext-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes [6]. We formally prove the security of HASBE based on security of the ciphertext-policy attribute-based encryption (CP-ABE) scheme by Bethencourt and analyze its performance and computational complexity. In data server user details, data requester details will be stored.

User details start will registration, user request and response details. Data requester will register and get login credentials so that data requester can request user location and response result will store in data server. Each user location details will be fetched using GPS device in the mobile. User latitude longitude details will stored then there securely in the location server based on attribute based encryption. Location user will be obtained only through admin only [7][8].

IV. CONCLUSION

Location based service can be used in a variety of contexts, such as health, indoor object search, entertainment, work, personal life, etc. Location based services is critical to many businesses as well as government organizations to drive real insight from data tied to a specific location where activities take place. The spatial patterns that location-related data and services can provide is one on its most powerful and useful aspect where location is a common denominator in all of these activities and can be leveraged to better understand patterns and relationships. Therefore, by using hierarchical level of database store we can provide secure data when sharing location based data to the trusted users.

V. REFERENCES

[1]. Xinlei Wang, Amit Pande, Jindan Zhu, and Prasant Mohapatra,*STAMP: Enabling Privacy-Preserving Location Proofs for Mobile Users, 2016.*

[2]. S. Saroiu and A. Wolman, *Enabling new mobile applications withlocation proofs,* in *Proc. ACM HotMobile*, 2009, Art. No. 3.

[3]. R. Steinbach, J. Green, and P. Edwards, *Look who's walking: Social and environmental correlates of children's walking in London,*HealthPlace, vol. 18, no. 4, pp. 917–927, 2012.

[4]. R.Hasan and R. Burns, *Where have you been? secure location provenance for mobile devices,CoRR* 2011.

[5] .B. Waters and E. Felten, *Secure, private proofs of location,* Department of Computer Science, Princeton University, Princeton, NJ, USA, Tech. Rep., 2003.

[6]. D. Singelee and B. Preneel, *Location verification using secure distance bounding protocols,* in *Proc. IEEE MASS*, 2005.

[7]. N. Roy, H. Wang, and R. R. Choudhury, *I am a smartphone and I can tell my user's walking direction,* in *Proc. ACM MobiSys*, 2014, pp. 329–342.

[8]. H. Han *et al., Senspeed: Sensing driving conditions to estimate vehicle speed in urban environments,* in *Proc. IEEE INFOCOM*, Apr. 2014, pp. 727–735.