IJRRECS/May 2015/Volume-3/Issue-5/3892-3896 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

IMPLEMENTATION OF EFFECTIVE MOBILE APPLICATIONS BY LOCATION SERVICES

S.Shreeha Tejaswini[1], C.Yosepu[2]

[1]M.Tech Student, Dept of CSE, St.Martin's Engineering College, Kompally, Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, St.Martin's Engineering College, Kompally, Hyderabad, T.S, India

ABSTRACT:

There are quite a lot of forms of mobile location based services. Although there have been quite a lot of researches on location privacy concerning general location-based services, they all enclose their limits. We have put forward an efficient and scalable privacy preserving location-based rewarding system, known as LocaWard. In this system mobile users accumulate location basis tokens from distributors of token and then redeem their assembled tokens at collectors of token for valuable rewards. The proposed design does not require any consistent server for generating location proofs for protecting privacy of user location. The system that was set up includes a trusted third party, token distributors of token, mobile users, a central controller and collectors of token. The completeness in addition to soundness of protocol was verified while the majority of previous systems only spotlight on their totality. We have projected a well-organized as well as privacy aware location based rewarding procedure for LocaWard system that mainly consists of initiation of identity, distribution of token as well as redemption of token.

Keywords: LocaWard system, Location based services, Trusted third party, Mobile users, Privacy preserving.

1. INTRODUCTION:

Due to rapid expansion of mobile devices, services on the basis of mobile location have come out as a novel form of mobile marketing. In generally among several forms of mobile location based services, one of them is location-based social networking where users allocate their locations with

friends [1]. Mobile commerce is another form which does not consider rewarding services. In recent times a novel category of mobile location based services known as location based check-in game, which is on the basis of location-based social networking, permits users to produce valuable rewards if they visit convinced places. Earlier works on user identity confidentiality in wireless networks are not valid to mobile location based services. Even though there have been several researches on location privacy concerning general location-based services, they all contain their limitations. In our work, we put forward a novel secure privacy preserving as well as practical location-based rewarding system, known as LocaWard, where mobile users can gather location-based tokens from distributors of token and then redeem their assembled tokens at collectors of token for valuable rewards. We propose a secured as well as privacy aware location based rewarding procedure for the projected system [2]. It mainly consists of three processes such as initiation of identity, distribution of token as well as redemption of token. The proposed design does not need any reliable server for generating location proofs for protecting privacy of user location. The completeness as well as soundness of protocol was verified while the majority of previous systems only spotlight on their totality.

2. AN OVERVIEW OF SYSTEM ARCHITECTURE:

The system that was introduced includes a trusted third party, token distributors of token, mobile users, a central controller and collectors of token. The trustworthy third party provides each mobile user with an actual identity as well as a corresponding certificate. The trustworthy third party is only accountable for issuing identities and not concerned in any other activities within system. An authorized mobile user is capable to get hold of token of location-based when it visits entity that contributes in the system. The tokens that are issued at different distributors of token contain the similar format but perhaps different indicated values. With all gathered tokens, a mobile user can redeem them for valuable rewards not only at similar store, but moreover at any other retailers. The quantity of received rewards depends on value that is represented by collected tokens. Besides, central controller accumulates token audition information sent by distributors of

token and provides it towards collectors of token when necessary. In the threat Model of proposed system, we consider that some outsider adversary within the network might intend to get hold of mobile user private information by means of impersonating several lawful mobile users or else eavesdropping on wireless communications [3][4]. In addition, as there are benefits of containing location-based tokens, mobile users have the motivation to lie towards distributors of token or collectors of token. First, they can produce extreme token requests in the direction of distributors of token and attempt to get hold of numerous tokens during same visit, or try to redeem the similar token more than once at collectors of token. Second, a mobile user might eavesdrop on communications between several mobile users and distributors of token and collectors of token steal their tokens and attempt to redeem the tokens. Third, a mobile user may alter the content of a token to attempt to get hold of more rewards. In LocaWard system distributors of token are trusted by collectors of token to offer applicable location-based tokens following their pre-established contracts. Collectors of token moreover trust distributors of token in the sense that distributors of token would not collude with mobile user to weaken their general interest [5]. We consider those distributors of token, a central controller and collectors of token work in semi honest approach that is they realistically execute system procedure, but are curious about privacy of mobile user.

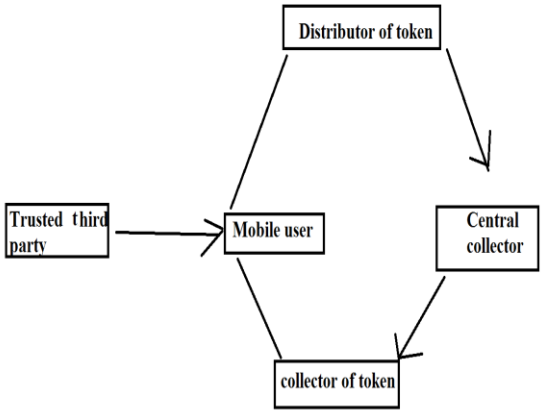

Fig1: An overview of proposed system.

3. AN OVERVIEW OF PRIVACY AWARE LOCATION-BASED REWARDING PROCEDURE:

We have proposed an efficient as well as privacy aware location based rewarding procedure for the projected system. In this system we assume that distributors of token, central controller and collectors of token work in semi-honest method, specifically they correctly carry out system procedure but are curious about privacy of mobile user, including their personal information. Protocol mainly consists of three processes

such as initiation of identity, distribution of token as well as redemption of token. In initiation of identity trusted trustworthy third party provides each mobile user with an actual identity as well as a corresponding certificate. Each mobile user keeps its identity private and produces a novel pseudonym for every token request or redemption. The certificate is employed for a user's identity authentication devoid of revealing its actual identity. In token distribution, a distributor of token needs to make sure if a mobile user requesting a token is an authorized user in system devoid of knowing its actual ID. Distributors of token issue an anonymous token which can be redeemed at any collectors of token for rewards. In token redemption, a collector of token verifies whether current mobile user trying to redeem a token is a legal system user, devoid of knowing its real ID. Collectors of token checks to see if token to be redeemed is intact and has not been altered as it was generated with central controller devoid of knowing content of token. Collectors of token checks if token does fit in to mobile user and he passes al verification phases, then collectors of token verifies whether value of token claimed by mobile user is true, and if so, allocate equivalent rewards. In proposed system, no one else other than trustworthy third party can recognize real identity of mobile user [6]. As the central controller and collectors of token only contain knowledge of token audition information, they do not make out the content of any token. As distributors of token and collectors of token is aware of location of tokens it accepted and there is no central server to accumulate the entire historical location information, no entity could figure out any specific mobile user location history.

4. CONCLUSION:

In our work we have introduced a system of LocaWard, which is a novel protected privacy preserving as well as realistic location-based rewarding system where mobile users accumulate tokens of location-basis from distributors of token and then redeem their assembled tokens at collectors of token for valuable rewards. The system includes a trusted third party, token distributors of token, mobile users, a central controller and collectors of token. In LocaWard scheme distributors of token are trustworthy by collectors of token to offer applicable location-based tokens following their pre-established contracts. We have

suggested a protected and privacy aware location based rewarding method for system containing three processes such as initiation of identity, distribution of token as well as redemption of token. The system does not need any reliable server for generating location proofs for protecting privacy of user location. The entirety as well as soundness of protocol was verified while the majority of previous systems only limelight on their totality. In the projected system we assume that distributors of token, central controller and collectors of token work in semi-honest process, particularly they accurately carry out system procedure but are curious about privacy of mobile user, including their personal information. In proposed organization, no one else other than trustworthy third party can recognize real identity of mobile user.

REFERENCES

[1] C. Ardagna, S. Jajodia, P. Samarati, and A. Stavrou, "Providing Mobile Users' Anonymity in Hybrid Networks," Proc. 15th European Symp. Research Computer (ESORICS), Sept. 2010.

[2] M. Gruteser and D. Grunwald, "Anonymous Usage of Location- Based Services through Spatial and Temporal Cloaking," Proc. First Int'l Conf. Mobile Systems, Applications Services (Mobisys '03), May 2003.

[3] B. Gedik and L. Liu, "Protecting Location Privacy with Personalized K-Anonymity: Architecture and Algorithms," IEEE Trans. Mobile Computing, vol. 7, no. 1, pp. 1-18, Jan. 2008.

[4] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing Location-Based Identity Inference in Anonymous Spatial Queries," IEEE Trans. Knowledge Data Eng., vol. 19, no. 12, pp. 1719-1733, Dec. 2007.

[5] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems (ICDCS), June 2005.

[6] H. Kido, Y. Yanagisawa, and T. Satoh, "An Anonymous Communication Technique Using Dummies for Location-Based Services," Proc. IEEE 25th Int'l Conf. Distributed Computing Systems (ICDCS), July 2006.