Mrunalini S. Kalamkar *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 11, November- 2014, pg. 176-178 **ISSN: 2321-8363**

Dynamic Linkability with User Authentication Privacy Preserving for Roaming Services: A Review

Mrunalini S. Kalamkar
III sem M.Tech CSE, Vidarbha Institute of Technology, Nagpur, India
Kal.mrunal@gmail.com

Prof. Pravin Kulurkar
Assistant Professor, Vidarbha Institute of Technology, Nagpur, India
pravin.kulurkar@gmail.com

Abstract: ***The roaming service enables mobile subscribers to access the internet service anytime and anywhere, which can fulfill the requirement of ubiquitous access for the emerging paradigm of networking, e.g., the Internet of Things (IoT). The existing system propose a conditional privacy-preserving authentication with access linkability (CPAL) for roaming service, to provide universal secure roaming service and multilevel privacy preservation Provides an anonymous user linking function by utilizing a novel group signature technique, which can not only efficiently hide users identities but also enables the authorized entities to link all the access information of the same user without knowing the user's real identity. Specifically, by using the master linking key possessed by the trust linking server, the authorized foreign network operators or service providers can link the access information from the user to improve its service, while preserving user anonymity, e.g., using individual access information to analyze user preferences without revealing user's identity. Furthermore, the subscribers can also use this functionality to anonymously query their usage of service. In addition, we propose to strong smart gateway for user authentication very efficiently. Through extensive analysis, we resists various security threats and provides more flexible privacy preservation compared to the existing schemes. Meanwhile, performance evaluations demonstrate its efficiency in terms of communication and computation overhead.***

Keywords: Internet of Things (IoT), conditional privacy-preserving authentication with access linkability (CPAL)

1. INTRODUCTION

WITH the advancements in various mobile and wireless networks, e.g., long-term evolution (LTE) worldwide interoperability for microwave access (WiMAX), and roadside-to-vehicle communication systems pervasive Internet access becomes a reality, enabling mobile subscribers (MSs) to enjoy Internet service anytime and anywhere. This also caters to the demand of ubiquitous access for the emerging paradigm of networking, e.g., the Internet of Things (IoT) which is rapidly gaining ground in the scenario of wireless telecommunications. Due to the complementary nature of the existing networks, inter working among them is attractive. However, within the heterogeneous networks, ensuring the secure and efficient roaming service is still challenging because different networks have different security policies and authentication protocols. Consequently, any secure roaming scheme dedicated for only one type of network technology cannot fulfill the security requirements from the heterogeneous networks. In heterogeneous networks, user privacy preservation has become an important and challenging issue in the roaming service, and has been widely studied by researchers. In most existing secure roaming schemes, the privacy preservation only equates with anonymity, i.e., hiding users' identities. However, this may not be suitable for diverse privacy requirements in real World. To this end, foreign network (FN) operators or service providers may need individual access information on the usage of services, while preserving anonymity. This means that FN operators or service providers can link all the access information of the same user for statistical purposes.

But they cannot know who the user is, what the current membership status of the user is, and the history of the user joining and revocation. Meanwhile, a user may want to provide a specific network operator or service provider with linking capability, and remain unlinkable to others. However, the existing secure roaming schemes do not support this function. This will significantly increase the burden of the home authentication server and potentially reduce the efficiency of the whole network. Therefore, efficient user revocation for dynamic membership in the secure roaming services is important.

Hence for overcome these issues we propose to strong smart gateway for anonymous user authentication, session key agreement, user tracking, and anonymous user linking are provided, which make the privacy preservation more flexible. And efficient revocation function for dynamic membership, where a group of users can be revoked simultaneously.

2. RELATED WORK

In literature, we study most of the recent conditional privacy-preserving authentication with access linkability (CPAL) for roaming service, to provide universal secure roaming service and multilevel privacy preservation. Provides an anonymous user linking function by utilizing a novel group signature technique,. [1]. first identify some unique design requirements in the aspects of security and privacy preservation for communications between different communication devices in vehicular *ad hoc* networks. We then propose a secure and privacy-preserving protocol based on group signature and identity (ID)-based signature techniques[2]. The proposed protocol is characterized by the generation of on-the-fly short-time anonymous keys between On-Board Units (OBUs) and Roadside Units (RSUs), which can provide fast anonymous authentication and privacy tracking while minimizing the required storage for short-time anonymous keys[3].With the recent introduction of mobility management frameworks in the IEEE 802.16e standard, the performance largely depends on the capability of performing fast and seamless handover between heterogeneous network proposed approach provides better performance and more exhaustive for enhancing VHO[4].

All these techniques tried to cover different issues maintaining the cost of implementation. Also there is lack of privacy and security in these techniques.

3. PROBLEM DEFINITION

Up till now, Foreign network (FN) operators or service providers may need individual access information on the usage of services. FN operators can link all the access information of the same user for statistical purposes. But they cannot know who the user is, what the current membership status of the user is, and the history of the user joining and revocation. Meanwhile, a user may want to provide a specific network operator or service provider with linking capability, and remain unlinkable to others. However, the privacy preserving. Unauthorized user can accent internal and external network .Data security in the roaming transmission.is not in existing secure roaming schemes do not support this function. This will significantly increase the burden of the home authentication server and potentially reduce the efficiency of the whole network. Therefore, efficient user revocation for dynamic membership in the secure roaming services is important.

4. PROJECT OBJECTIVES

The objective of proposed techniques is
- To help the foreign network know who the user is, what the current membership status of the user is, and the history of the user joining and revocation.
-To detect unauthorised user by log monitoring.
-To find out internal as well as external attack.

-To reduce time for data transferring one network to other network and also making strong security and privacy in roaming network.

5. INVESTIGATIONAL OUTCOME

To achieve the objective of this project, we have proposed following techniques :
- We will create a smart gateway between the two end user for detecting user is authorised or not.
-For security we will implement AES algorithm.
- And for id we use user random id generation technique.
-For user tracking we will monitor the log of user.

6. CONCLUSION

This review paper proposes a technique to strong smart gateway for anonymous user authentication, session key agreement, user tracking, and anonymous user linking are provided, which make the privacy preservation more flexible. And efficient revocation function for dynamic membership.

REFERENCES

[1] Chengzhe Lai, Hui Li, Xiaohui Liang,and Rongxing Lu, "CPAL: A Conditional Privacy-Preserving Authentication With Access Linkability for Roaming Service" IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, FEBRUARY 2014
[2] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS:Asecure and privacy-preserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007
[3] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. IEEE INFOCOM, 2008, pp. 1229–1237
[4] Rupam Deb, and Kazi Rafiqul Islam " Performance Improvement of Seamless Vertical Handover in Heterogeneous Wireless Network" IEEE international conference on communication system and network technology.
[5] A. Al Shidhani and V. Leung, "Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers," IEEE Trans. Dependable Secure Comput., vol. 8, no. 5, pp. 699–713, Sep./Oct. 2011.
[6] F. Xu, L. Zhang, and Z. Zhou, "Interworking of WiMAX and 3GPP networks based on IMS [IP multimedia systems (IMS) infrastructure and services]," IEEE Commun. Mag., vol. 45, no. 3, pp. 144–150, Mar. 2007.
[7] P. Taaghol, A. Salkintzis, and J. Iyer, "Seamless integration of mobile WiMAX in 3GPP networks," IEEE Commun. Mag., vol. 46, no. 10, pp. 74–85, Oct. 2008.
[8] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.
[9] L. Tan and N. Wang, "Future internet: The internet of things," in Proc. 3rd Int. Conf. Adv. Comput. Theory Eng., 2010, vol. 5, pp. 376–380.
[10] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's INTRAnet of things to a future INTERnet of things: A wireless-and mobility-related view," IEEE Wireless Commun., vol. 17, no. 6, pp. 44–51, Dec. 2010.

