Multiple user Link with user privacy preserving and Authentication for Roaming Services: A Review

Mrunalini S. Kalamkar,
2nd year Mtech CSE, Vidarbha Istitute of Technology, Nagpur, India.
Kal.mrunal@gmail.com

Prof. Pravin Kulurkar,
Assistant Professor, Vidarbha Istitute of Technology, Nagpur, India.
pravinkulurkar@gmail.com

Abstract

The roaming service communication is difficult part to one network to another network. The main server having all services for provide or communicate to other. while during this communication we must secured the data or its privacy preserve. hence we propose to strong smart gateway for both network to user authentication very efficiently, and doing its services very easily with efficiently hide users identities and for security we applying AES algorithm is good result compare to exiting system i.e Novel Group Signature Technique(NGST) in conditional privacy-preserving authentication with access linkability (CPAL) ,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: Novel Group Signature Technique(NGST),Conditional Privacy-preserving Authentication with access Likability (CPAL)

1. INTRODUCTION

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). 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 of the same user for statistical purposes. The existing system having this limitation like 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. 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. And in proposed system we also applying a AES algorithm for data encryption is most secured as compared to existing NGST technique.

2. . RELATED LITERATURE

In literature, we study the recent conditional privacy-preserving authentication with access likability (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]. 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. [3] 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. [4]. All these techniques tried to cover different issues maintaining the cost of implementation. and there is lack of privacy and security in these techniques.also we applying all services working efficiently by the help of getaway i.e. admin are in all network its check the user authentication .

3. PROBLEM DEFINITION

Roaming network (RN) operators or service providers may need individual access information on the usage of services. but this is very risky job to knowing all the information of other network. However, the issue in privacy preserving of user is happening . in existing system Unauthorized user can accessing internal as well as external network. hence the security problem in the existing system is occurred for not having any smart gateway. and data is not in encrypted form for transmission. However reduce the efficiency of the whole network.

4. PROJECT OBJECTIVES

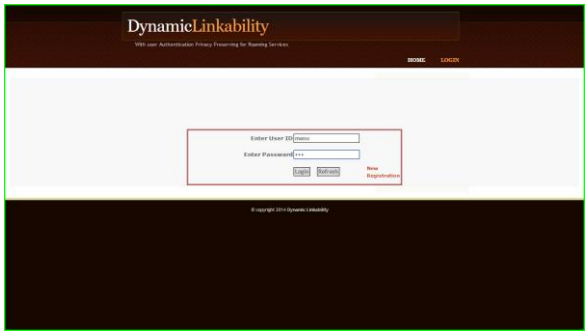
The objective of proposed techniques is
- Help of the gateway i.e. admin of network record like to know who the user is, what the current membership status of the user is, and the history of the user joining and revocation , from where he come.- We create a smart gateway between the two end user for detecting user is authorised or not.
-To find out local as well as roaming network user attack.
-To detect outer user or unauthorised user by log monitoring.
-To grow security and privacy with the help of algorithm in roaming network.
-For user tracking we will monitor the log of user
-For security we will implement AES algorithm.
- And for id we use user random id generation technique.

5. INVESTIGATIONAL OUTCOME OF PROPOSED WORK

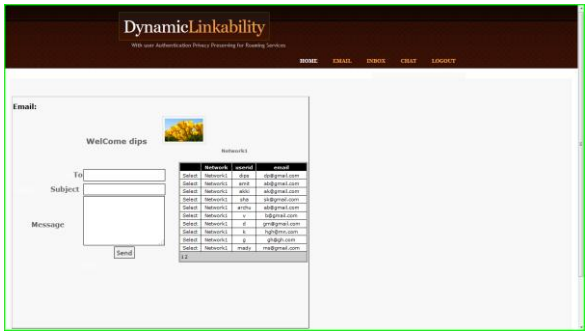
In this paper we made a one network having a all services like email to local network , inbox, chatting services to roaming network. Then 1st client register to admin. admin check its background then approved its authorised user .admin maintain all authorised user information of local network and roaming network.

In inbox service show the message of local network or roaming network.in message show the time of reach, subject, message, status etc.

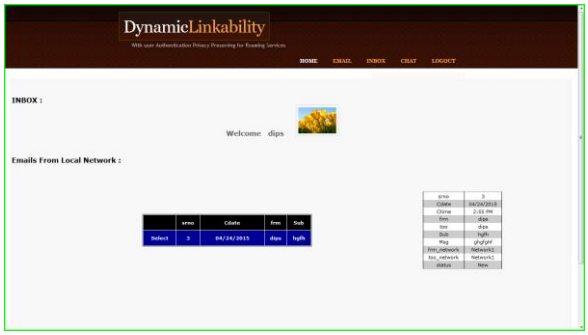
Chatting is the service in network 1 and network 2 these network communicate through chatting service but for chatting firstly network 1user verification request to admin of network 1 it got then go to for approval to network 2 admin. admin gave a approval for chatting then start the chatting of two roaming network user.



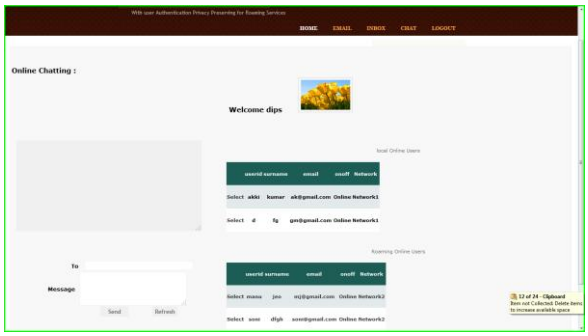
User Login



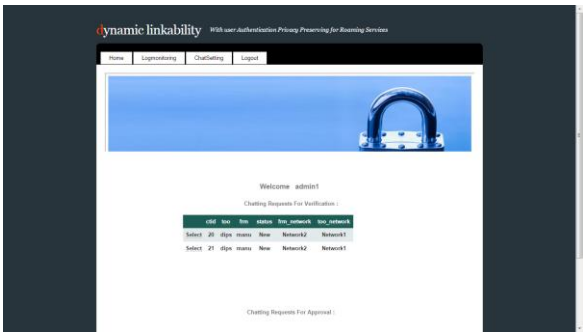
User Emailing Service on a local Network as Network 1.



UserInbox On a Local Network

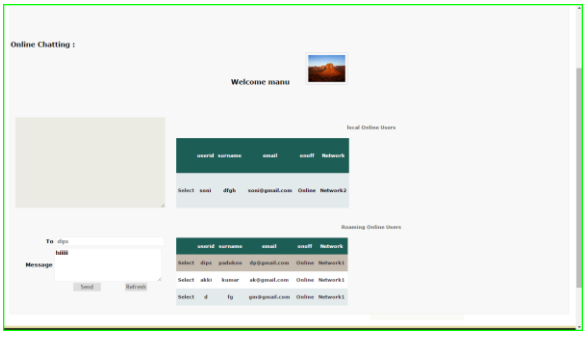


User Chating Approval For Chatting On a Remote Roaming Network



Successfully Verification :

Successfully Approved By Roming Network Admin:



Now User1 Send chating Msg to user2:

6. CONCLUSION

This paper proposes a strong smart gateway to more than one network for anonymous user authentication, user tracking, session key agreement, make the privacy preservation more flexible. its find out internal as well as external attacks. with the help of AES algorithm data encryption transmission is very secured. Email services in local and chatting services in roaming network is work efficiently.

7. 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.

[11] Ms.Mrunalini Kalamkar, Prof. Pravin Kulurkar "Dynamic Linkability with user Authentication privacy preserving for Roaming Services:A review" International journal on computer science and mobile applications, vol.[12] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preservingopportunistic computing framework for

mobile-healthcare emergency,"IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 3,pp. 614–624, 2013.[13] D. He, C. Chen, J. Bu, S. Chan, and Y. Zhang, "Security and efficiencyin roaming services for wireless networks: challenges, approaches,andprospects," IEEE Communications Magazine, vol. 51, no. 2, pp. 142–

150, 2013.