Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Anonymous Authentication Scheme for Mobile Crowd Sensing

Kad Pradnya Dinkar, S A Jain
Department of Computer Engineering, Savitribai Phule Pune University,
Pune, Maharashtra, India

Abstract— Anonymizing network gives anonymous access to their users by hiding their IP address. In anonymizing network users share their data with another network services, for accessing one user to other user data communication process. User behaviour is main task in present days. For observe this of task efficiently, nymble a misbehaving user detection mechanism can be developed. Mobile crowd sensing (MCS) is one of the major trends which plays vital roles in areas such as traffic monitoring and commercial advertisements by taking data shared by users by analysis. Major concern in MCS is data transitions may lead to leakage of private data such as IP address and identities, when they share their data to third parties. In this paper we give how we provide anonymous authentication scheme to the user who share their important data to any third party.

Keywords— Anonymizing network, Mobile crowd sensing, IP address, User analysis, Anonymous authentication,

I. INTRODUCTION

Anonymizing network is use to protect privacy and identity of the users, giving them anonymous access to services provided by many web servers. If any user misbehaves, taking advantage of anonymity, the site administrators have to block complete anonymizing network because they can not find and block particular misbehaving user. Nymble, the base system used to solve such type of problem. It maps user's system IP address by pseudonym and assign ticket for them to give anonymous access to servers. This Anonymous authentication is apply for many area like mobile crowd sensing (MCS). The increasing use of sensors on today's smart phones has already opened up new possibilities for collecting sensed information from environment. Mobile crowd sensing apply to the huge varity of sensing model in which particular with sensing and computing devices are capable to gather and grant important data for third parties. MCS can be spread out on many field of applications, such as health monitoring, traffic monitoring and so on. Following figure 1 shows many field of application of MCS.

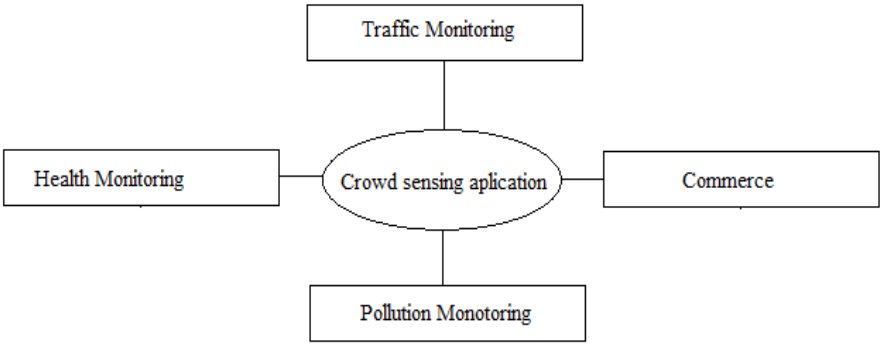

Fig.1 crowd sensing application

MCS applications can be used to able a broad spectrum of applications, ranging from monitoring the pollution condition or location based services to monitoring traffic conditions. Assigning cover of safety and secrecy of exchanging information in MCS turn to develop attention from the industry and academia since the sensing data are usually sensitive for participants or users. Most of the time users take care regarding the destruction of their secrete data when they share their data to any third parties. To target on such problem, propose a blacklist based anonymous authentication scheme in which participants can enjoy an anonymous environment and allow their data without worrying about any data leakage. We apply anonymous authentication scheme to mobile crowd sensing for the purpose of security and privacy.

II. EXISTING SYSTEM

Existing system does not provide lots of security. Anonymous users can change their IP address and also flood may come to the network. Some site such as Wikipedia can not control this kind of misbehaving users or participants, so website get users IP address and block that misbehaving IP addresses. Below the shell of privacy, many times users damaged popular web sites as we can say in previous such as Wikipedia. When any particular user misbehave at that time site administrator can not blacklist one particular user's IP address they block the entire anonymizing network. In other words, a few "bad onion" can spoil the other one. But through anonymous user routing the IP address and use proxy

server or some other IP changing software user can enter into network. This system having such type of limitations which degraded our performance.

Disadvantages

- Blocking system does not provide security.
- Any user can change IP and enter into network.
- There is no way to stop anonymity in such type of system and website admins can block only fake IP.

III. PROPOSED SYSTEM

The present system provide several solution on existing system problem, each provide some degree of liability. In pseudonymous credential systems if user misbehave they should added into the blacklist. Anonymous credential systems employ group signatures. Basic group signature permit servers to dismiss a misbehaving use's anonymity by complaining to a network manager. Server must query the network manager for every authentication, and thus lacks accessible. We show main entities involved in our scheme those are as follow.

- Participant
- Pseudonym Manager (PM)
- Application Provider (AP)
- Network Manager (NM)

Following figure 2 shows model for anonymous authentication scheme which focus on main four entities of it.

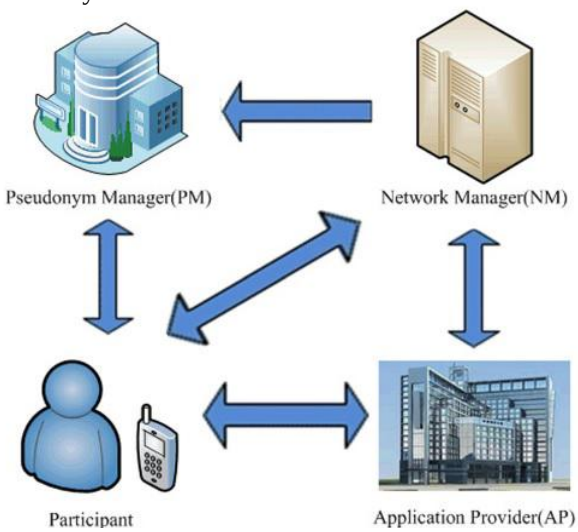

Fig.2 model for anonymous authentication scheme

Participant: Using sensors on everyday devices, such as personal digital assistant(PDA), phones participant share their important data to the application provider. Participant with identity uid must register with the PM i.e. pseudonym manager once in each linkability window. Transaction is divided into linkability window of duration w, each of them is divided into m transaction identifiers. A participant must register once in each linkability window, after accessing to application provider m times, participant must have to register again. When participant or we can say user share their information about subject of interest to the application provider, but before that they must have to get pseudonym form the pseudonym manager.

Pseudonym Manager (PM): During System initialization NM interacts with other entities. Firstly, NM generates a number of private keys for the system. This private keys are used to generate the pseudonym and verify the integrity of pseudonym for NM, and then NM issues it to PM through a secure communication channel. Participant must first contact the pseudonym manager and confirm control over a resource; for IP address blocking, participant is required to connect to PM directly. This pseudonym is require for participant for get access of different application also. PM only knows participant or user identity-pseudonym pairs.

Application Provider (AP): Application provider not only provide services to participant but also manage reputation score of participant. They manage scoring grades, updating scores and modifying scores also. Application provider manage blacklist of misbehaving participant, because of it we can predict participant's authority for enjoying anonymous environment. Application provider set policies that each participant have to satisfy. Each provider may register at most once in linkability window.

Network Manager (NM): Network manager is in charge of maintaining and computing the participant's current scores and generating the participant's credential in order to authenticate with application provider. NM having control center of the system. After getting pseudonym from the PM , participant connect to the network manager through anonymizing network. Network manager only knows the pseudonym-server pair. They are place between this two entities. NM knows which application provider, particular participant wants to contact, but other information such as participant's IP address is kept unknown.

Advantages: System having certain advantages such as follow,

- Instead of getting real indentity, adversary can get only pseudonyms of participants.
- Nonrepudiation is one of the property of the system through which participant can not deny that he has accessed the service provided by application provider.
- Participant who is in blacklist he can not access anonymous service. Blacklist is maintain such misbehaving participant.
- Provide unlinkability through which not leak any information to an adversary by allowing them to trace it.

IV. CONTRIBUTION OF THIS PAPER

Blacklisting misbehaving users: Through anonymous authentication we can prevent malicious user's misbehaviour. Participant's score are manage by application provider, also provide a series of policies that participant's reputation scores must satisfy. If their score not satisfy then they will be added in the blacklist.

Assign score to participants: Measure participant's access authority by their scores which is scored by application provider. Application provider assign positive or negative score to each and every user according to their behaviour.

Efficiency: This system use huge take over only if its behaviour is acceptable at the server. This makes use of inexpensive symmetric key encryption to achieve anonymous authentication instead of public key encryption.

V. CONCLUSIONS

In this paper we motivated the need of anonymous authentication scheme when private and valuable information is share to third party. Utilized the blacklist technique to propose a practical anonymous scheme to preserve privacy of participant when they make access to terminal. System support anonymous blacklisting relying on trusted third parties that are capable of linking users. Provide symmetric key encryption through which achieve anonymous blacklisting, anonymity, nonrepudiation and unlinkability.

ACKNOWLEDGMENT

The authors are grateful to Department Of Computer Engineering MIT Academy Of Engineering Pune, Alandi(D) for suggestion and their guidance.

REFERENCES

[1] R. A. Haraty, B. Zantout, "The TOR data communication system," IEEE communication and networks, vol 16, pp. 415-420, 2014.

[2] S. Malgaonkar, Y.B. Nag, G. Damle, "Implementation of optimized nymble system to enhance network security," IEEE international conf. on computational intelligence and computing research, pp. 1-6, 2013.

[3] Jen-Ho Yang, Chin Chen Chang, "An ID-based remote mutual authentication with key agreement schemes for mobile devices on elliptic curve cryptosystem," ScienceDirect, 2008.

[4] Li H, Yang Y, Wen M, Luo H, Lu R, "Emrq: An efficient multi keyword range query schemes in smart grid auction market," KSII Trans. Internet Inf Syst., 2014.

[5] Yang Y, Li H, Wen M, Luo H, Lu R, "Achiving rank range query in smart grid auction market,", In: IEEE International Conference On Communications (ICC).

[6] Li H, Lin X, Yang H, Liang X, Lu R, Shen X, "EPPDR: An efficient privacy preserving demand response scheme with adaptive key evolution in smart grid," IEEE Tranc. Parallel Distrib Syst 25(8): 2053-2064, 2014.

[7] A. Lysyanskaya, R. L. Rivest and A. Sahai, " Pseudonym systems: selected area in cryptography," LNCS 1758, pp. 184-199, Springer.

[8] P.P. Tsang, A. Kapadia and Smith, "Blacklistable anonymous credentials:blocking misbehaving users without TTP's," Proc. 14th ACM Conf. computer and comm. Security (CCS'07), pp. 72-81, 2007.

[9] J. Camenisch and lysyanskaya, "Signature scheme and anonumous credential from bilinear maps," Proc. Ann.Int'1 cryptology conf. (CRTPTO), Springer, pp. 56-72, 2004.

[10] R. Ravikarthik, R. Jebakumar, "Blocking misbehaving users using nymble system ," International Conference on Computing and Control Engineering 12 &13 April, 2012.

[11] Kamble Maheshkumar S, Prof. Hatkar S. S, "Blocking of Mischievous Users in Anonymizing Networks Using Nymble System: A Survey Study", Elsevier,2010.

[12] Cheung M, Hou F, Huang J, "Participation and reporting in participatory sensing", the 12th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), pp 357–364, 2014.

[13] Liu D, Li H, Yang Y, Yang H , "Achieving multi-authority access control with efficient attribute revocation in smart grid", In: IEEE International Conference on Communications (ICC). IEEE,pp 634–639, 2014.

[14] Mianxiong D, Kimata T, Sugiura K, Zettsu K, " Quality of experience (qoe) in emerging mobile social networks", IEICE Trans Inf Syst 97(10):2606–2612,2014.

[15] P.C.Jonson, A. Kapadia, P. P. Tsang and S.W.Smith "Nymble anonymous IP address blocking ," In Privacy Enhancinh Technologies, LNCS 4776, pp. 113-133, Springer, 2007.

[16] Yang Y, Li H, Liu W, Yang H, Wen M, " Secure Dynamic Searchable Symmetric Encryption with Constant Document Update Cost", In: Proceedings of GLOBECOM. Anaheim,California, USA, 2014.

[17] Ota K, Dong M, Chang S, Zhu H, "Mmcd: Max-throughput and min-delay cooperative downloading for drive-thru internet systems", In: IEEE International Conference on Communications (ICC). IEEE, pp 83–87, 2014.

[18] Talasila M, Curtmola R, Borcea C, "Improving location reliability in crowd sensed data with minimal efforts", In: The 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC).IEEE, pp 1–8, 2013.

[19] Ganti R.K., Ye F, Lei H "Mobile crowdsensing: current state and future challenges. IEEE Commun Mag 49(11)32-39, 2011.

[20] Ota K, Dong M, Zhu H, Chang S, Shen X, "Traffic information prediction in urban vehicular networks: A correlation based approach", In: IEEE Wireless Communications and Networking Conference (WCNC). IEEE, pp 1021–1025, 2011.

[21] Tsang PP, Au MH, Kapadia A, Smith SW, "Blacklistable anonymous credentials: blocking misbehaving users without ttps", In: Proceedings of the 14th ACM conference on Computer and communications security, pp 72–81,2007.

