Blacklisting User In Mobile Crowd Sensing

Kad Pradnya Dinkar[1], Prof. S A Jain[2]

[1] *ME Student Computer Engineering, MIT Academy Of Engineering, Maharashtra, India*
[2] *Professor ,Dept. of Computer Engineering, MIT Academy Of Engineering, Maharashtra, India*

---***---

Abstract - *An Anonymizing network provide anonymous access to their participants through 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 performance is main task in current days. For observe this of task efficiently, nymble a misbehaving user sensing mechanism can be developed. Mobile crowd sensing (MCS) is one of the concept which plays important roles in different areas such as monitoring traffic and health monitoring by taking data shared by users by analysis. Major concern in mobile crowd sensing is data transitions may lead to leakage of private data such as IP address and identities, when they share data to any third entity. In this paper we give how we provide anonymous authentication scheme to the user who share their important data to any third party.*

***Key Words*: Anonymizing network, Mobile crowd sensing, IP Address, Nymble, Anonymous Authentication.**

1.INTRODUCTION

Anonymizing network is use to protect identity of the participants, providing them anonymous access to services provided by number of web servers. In case if participant not, taking advantage of anonymity, site controller have to keep restriction on complete anonymizing network because they can not identify and block particular misbehaving participant in respective network. System does not giving security and the anonymous participant can change their IP address and enter into the network which may spam the website. Some site such as Wikipedia not control such kind of behavior of participant, because of that the website retrieve participants IP address and block access of that misbehaving IP addresses. But anonymous participants routing the IP address and through some other IP changing software they can enter into particular network. Such system not offer security, so any participant can change IP and enter into particular network.

Nymble, the base system used to solve such type of problem. It maps users 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). Mobile crowd sensing apply to huge category of sensing model where particular with sensing, computing devices capable for gathering and grant important data for another entities. Mobile crowd sensing can be spread out different field of applications, like health monitoring, traffic monitoring and so on. Following fig.1 shows many field of application of MCS.

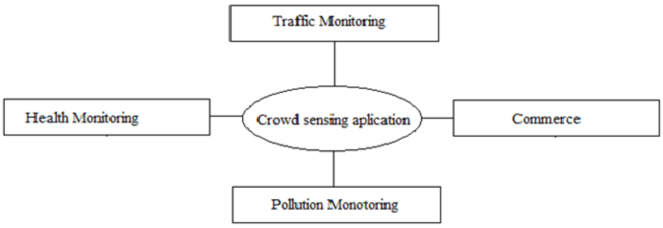

Fig -1: Crowd sensing application

MCS applications can be used to enable a broad spectrum of applications, ranging from monitoring the air pollution condition or location based services to monitoring traffic conditions or social network applications to a tasking entity such as a cloud service, where these data are aggregated, processed and remain available for third parties.

2. RELATED WORK

In [1], developed pseudonym credential system. In this type of system user uses pseudonym which is fake identity or fake name for logging into the website. These pseudonym are generated by tor client program. This system is not much computational and it is easier to implement but at the same time it having some disadvantages also like system having weaker anonymity. In [2], proposed ID- based remote mutual authentication with key agreement scheme on elliptic curve cryptosystem(ECC). It introduced elliptic curve cryptosystem to reduce computation loads for mobile devices. Most ECC scheme are based on public key cryptosystem. For prove validity, public key in the system requires the associated certificate. System support a session key agreement between participant and service provider.

In[3], involved new concept called anonymous credential system which consist with users and service provider. This system having concept of group signature they also consist of three parties namely an authority, verifier and user. Authority is permission given by the system for accessing different services provided by the system. In verifier step verify participants behavior and user is any respected one who want to access services. This system operate with group signature approach.

In[4], proposed that few of nymble system removed existence of the trusted party by improving anonymous credential system they name it as blacklistable anonymous credential system. It uses scheme which stands for the signature proof of knowledge scheme. After comparison system is more robust, scalable and support subjective authority [5]. When size of blacklist grows, blacklist checking cost and authentication computation cost with verification also increases. In anonymizing network even we provide security for protect user identity by using some technique like IP changing software, also flood may come to the network any third user may perform invalid task against system head. Previous system does not provide lots of security.

3. PROPOSED WORK

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

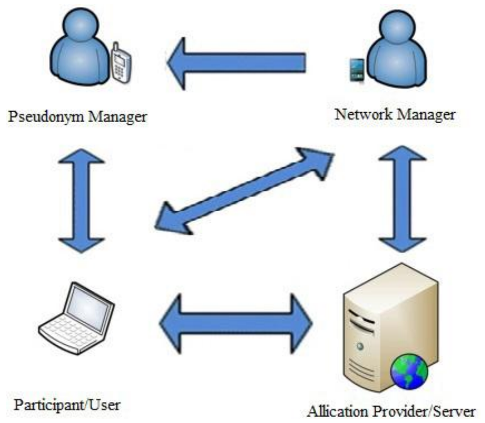

Fig -2: System model for anonymous authentication scheme

Participant: It is the entity that measures and shares required data about subject of interest to application provider by using sensors on everyday devices such as smartphones or personal digital assistant. How-ever, not all participants are always honest. Since, some participants may be misbehave. Participants are responsible for collect and upload data which is sensed.

Pseudonym Manager: Pseudonym Manager is in charge of mapping the participant's resources ID (example IP Address, MAC Address) to the pseudonyms. Pseudonym manager is the first entity that participant must contact, which determines whether the participant is permitted to register or not. Pseudonym Manager's duties are limited to determining the right of register and mapping IP address to pseudonym.

Application Provider: Application Provider not only provides the services to the user but also manages the reputation scores of a participant's including scoring grades, updating scores, and modifying scores. Application Provider maintains a blacklist which is used to determine participant's right of enjoying the anonymous environment of MCS. Application Provider lays down the policies that each participant must satisfy.

Network Manager: Network Manager is the control center of the system. Network Manager initiates the system parameters such as secret keys and secure hash functions and issues them other entities. Network Manager is in charge of maintaining and computing the participant's current scores and generating the participant's credentials in order to authenticate with Application Provider.

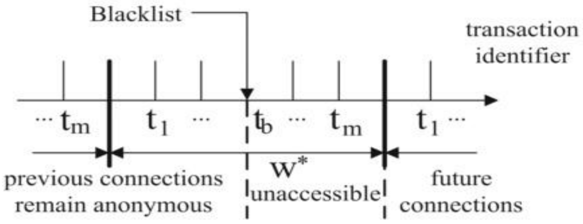

Fig -3: Linkability window

As shown in above fig. 3 transaction is divided into this window of duration w. When network manager maintain score of participants they consider some factor like identity of participant, previous score and transaction .

4. MATHEMATICAL MODEL

4.1 Set Analysis

In this section represent system in following mathematical way so, let S be the system, S = {Q, I, F, R, F0} Each of S, Q, I, F, R, F' are specified in follow.

- Q is the Set of Inputs.

Q = x : x is a resource

- I is the Initial State.

I = {r1}

r1 will be given as input initially

- R is the set of Intermediate States.

R = {R1, R2, R3} where,
R1 ={q1}, R2 = {q2}, R3 = {flag}
q1 = {x} x is a pseudonym received from pseudonym manager.
q2 = {x} x is a nymble ticket received from nymble manager.
flag = {x} x is an integer indicating granted access to server.

- F0 = Failure state.

R4 this state will be reached when a malicious activity is detected and a user is blacklisted.

- F=Final State.

R3 in this state the access will be grant to the user by server.

- Venn Diagrams: Represent this diagrams in fig. 4 to fig. 7 for this system.

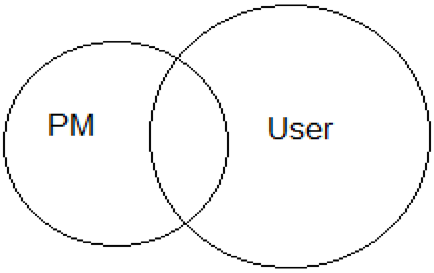

Fig -4: Pseudonym manager U user

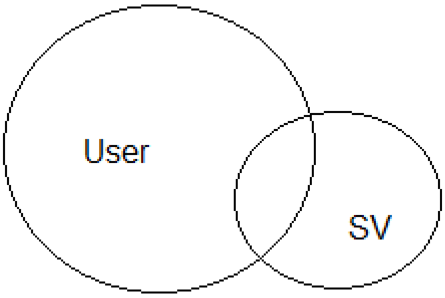

Fig- 5: User with Server

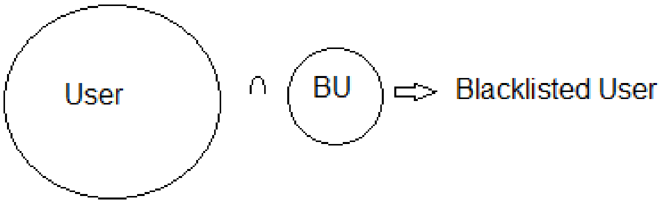

Fig- 6: User Intersection with blacklisted user

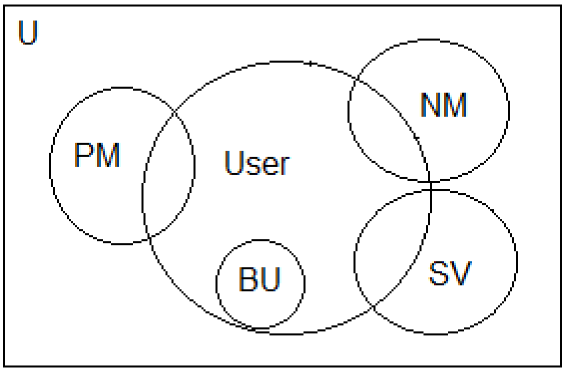

Fig- 7: Overall System

U: Universal set representing the network, which consists of the users, servers, pseudonym manager and the nymble manager.

PM: Set of pseudonym managers in the network.
PM = {x : x is a pseudonym manager}

NM: Set of nymble managers in the network.
NM= {x : x is a nymble manager}

USER: set of anonymous users in the network.
USER = {x : x is a user}

SV: set of servers to which users request for access.
SV= {x : x is a server}

BU: set of blacklisted users in the network.
BU= {x : x is a blacklisted user}

4.2 Related Phases

There are different phases like system initialization, participant registration, authentication. System work divided into different steps and goes through this phases in following manner.

Step 1: System Initialization
During System initialization network manager interacts with other entities. First, network manager generates a number of private keys (NPmackey) for the system. Private key NPmackey, which is used to generate the pseudonym for pseudonym manager.

Step 2: Participant Registration
Participant use ticket requested from network manager to authenticate. For that purpose we have to create pseudonym for participant. We create pseudonym in following way.

- Create Pseudonym

Algorithm 1: PMCreatePseudonym
This algorithm is use to generate pseudonym for participants
1) Take participant user id as (pid). pseudonym manager secret key (PMkey) and current linkability window (w).

2) Extract secret key (NPmackey) used to generate pseudonym for network manager.
3) For generation of pseudonym we having two component knym and kmac. Generation of both of them in below manner.

Knym= (pid, w, pmKey) (1)
Kmac= (knym, w, NPmackey) (2)

4) Return pseudonym (pnym)= (knym, kmac)
For generation of pseudonym we having two component knym and kmac.
Verify Pseudonym and Generate Ticket. Participant must have to register to network manager to get ticket to authenticate.
Participant send pnym and ids. ids is nothing but identity of application provider. Network manager accept pseudonym and check freshness
and integrity.

Algorithm 2: NMVerifyPseudonym
This algorithm is used to verify respected pseudonym
1) Take secret key share between network and pseudonym manager.
2) Check pseudonym as,

(knym, kmac)= pnym (3)
return kmac= (knym, w, NPmackey) (4)

Algorithm 3. NMCreateCredential
This is used to create credential to the system

1) Take pnym where pseudonym manager mapping participants resources identity to pnym.
2) Take server identity (ids) ,w, score (skr).
3) Encrypt (pnym, ids, w, skr) withkey (NAkey) share between network manager and application provider such as,

Ticket(tkt)= encrypt (pnym,w, ids, skr) (5)
Credential(crd)= tkt (6)

4) Generated crd is use for authentication.

Step 3: Authentication
Participant send their ticket to application provider if participant reputation satisfy then application provider pass authentication. In authentication phase focus on check whether user is blacklist or not, check freshness of user ticket, according to that decide whether add participant to the blacklist or not.

Practical reputation scores: We have to measure the participants access authority by his behavior scores which is scored by application provider. Application provider can score each user with positive or negative score with category identifier.

Blacklisting malicious users: Proposed technique that can prevent the malicious user's misbehavior. In this scheme, the application provider provides a series of policies that participant's reputation score must satisfy. Otherwise, participant's will be added to blacklist. Participant cannot enjoy the anonymous environment of MCS and in this scheme, we can add misbehaved users to blacklist using their pseudonyms instead of their real identity.

This scheme takes full consideration of computational ability of mobile devices. This proposed scheme is mainly based on symmetric key encryption instead of cost heavy public key encryption.

5. CONCLUSIONS

In this paper we proposed using blacklist based anonymous authentication scheme for mobile crowd sensing, system provide an authentication scheme to preserve privacy of participants of mobile crowd sensing when they make access to terminals. It also describe the proposed scheme can satisfy the desirable security requirements.

ACKNOWLEDGEMENT

I am very thankful to Prof. S A Jain for guiding and helping me for the project related information and give valuable comments. He helps me with a broad range of issues from giving me directions, helping to find solutions, outlining the requirements. I am furthermore thankful to other professors, Department of Computer Engineering to encourage me to go ahead and for continues guidance.

REFERENCES

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

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

[3] P. P. Tsang, A. Kapadia, and Smith, "Blacklistable anonymous credentials: Blocking misbehaving users without TTPs," Proc. 14th ACM Conf. computer and comm. Security (CCS07), pp. 72-81, 2007.

[4] 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.

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

[6] 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.

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

[8] Li H, Yang Y, Wen M, Luo H, Lu R, Emrq, "An efficient multikeyword range query scheme in smart grid auction market," KSII Trans Internet Inf Syst.,2014.

[9] Yang C, Ma W, Wang X, "Novel Remote User Authentication Scheme Using Bilinear Pairings In: Autonomic and Trusted Computing," Springer, pp. 306-312, 2007.

[10] Anil Kumar, Kirti Bhatia, "Blocking of Mischievous users in Anonymizing Networks using Nymble System," International Journal of Computer Science Communication Volume 6, Issue 2,2015.

[11] Patrick P. Tsang, Man Ho, Apu Kapadia, Sean W, Smith, "Blacklistable Anonymous Credentials: Blocking Or Misbehaving Users Without TTPs," USA October 29 November 2, 2007.

[12] Aryan Chandrapal Singh, Wavhal Dnyaneshwar N. Tambre Keshav G, "Misbehaving User Detection using Nymble Counter Measures in Anonymization Networks," International Journal of Advanced Research in Computer Science and Software Engineering, 2014.

[13] Wazir Zada Khan,Yang Xiang, Quratulain Arshad , " Mobile Phone Sensing Systems: A Survey," IEEE Communications Surveys Tutorials, Vol.15,2013.

[14] Raghu K. Ganti, Fan Ye, Hui Lei,T. J. Watson Research Center, "Mobile Crowdsensing:Current State and Future Challenges," IEEE 2011.

[15] Yang Y, Li H, Wen M, Luo H, Lu R, "Achieving ranked range query in smart grid auction market," In: IEEE International Conference on Communications (ICC). IEEE, pp 951956, 2014.

[16] 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 Trans Parallel Distrib System 25(8):20532064,2014.

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

[18] P. P. Tsang, A. Kapadia, and Smith, "Blacklistable anonymous credentials:Blocking misbehaving users without TTPs," Proc.14th ACM Conf. computer and comm. Security (CCS07), pp.72-81, 2007.

[19] J. Camenisch and A. Lysyanskaya, "Signature scheme and anonymous credential from bilinear maps,, Proc. Ann. Int 1 cryptology conf. (CRYPTO), Springer, pp. 56-72, 2004.

[20] R. Ravikarthik, R. Jebakumar, "Blocking Misbehaving Users Using Nymble System," International Con-ference on Computing and Control Engineering 12 13 April, 2012.