ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

Private Set Instruction for Secure Interest Sharing Computation Mechanism in Mobile Networks

[1]MOHIT CHAUHAN, [2]NISHANT NEGI, [3]AKSHANSH SINGH, [4]M.SENTHIL,
[1]UG Scholar, CSE Department, SRM University, Chennai
[2]UG Scholar, CSE Department, SRM University, Chennai
[3]UG Scholar, CSE Department, SRM University, Chennai
[4]Assistant professor, Dept.of CSE, SRM University, Ramapuram Campus ,
Senthil.m@rmp.srmuniv.ac.in
Email: [1]mhtchhn12@gmail.com,
[2]nishantnegi.0@gmail.com, [3]pradhanudayan@gmail.com,
Contact Number: +91-9940380760[1], +91-9940398600[2], +91-8939201540[3]

I) Abstract: In an age of interconnected global mobile networks and finding users who share common interest becomes a must. We live in a connected world but the fundamental back bone for this paradigm suffers from the inconsistency of over-reliance on trusted-third parties and secure servers. But user search based on common interest constraints leaves tremendous room for malicious agents to hijack the entire match making process. Therefore, a system needs to be proposed which allows secure and ubiquitous social connectivity through common interest. Furthermore, the computation mechanism does away with the need for secure servers and inherently provides a solution for implementation in mobile networks.

Index Terms: Interest Sharing, Social Network, Dummy interest, Random QBE.

II) Introduction:

With the rapid development of social networks, new associative patterns based on user interests have emerged and achieved prosperity for further study. The social graph reflects the people who have intimate contact with the user through a variety of ways and share common interests. Mining the interest structure in a large scale network has the tendency to unearth activity patterns. For example, people may want to ensure anonymity while sharing sensitive afflictions; which can be achieved by providing adequate security.

Along with the popularity of social networks the increasing danger of privacy breaches due to user location exposures. The motivation for the mechanism is to provide the user with a way to effectively share interests without the threats of malicious intentions. The challenge is that the concept of privacy may change significantly due to the contexts and location, user's behavior and many other factors.

In general, there are two straightforward ways to implement matchmaking in mobile networks. One way is a device to broadcast its owners profile information to the public for example using Bluetooth. This approach is risky as it leaks users' private information to anyone in the users' proximity. The second is to make used of trusted third party or secure servers; many times not viable due to cost factor. The proposed privacy preserving protocol for mobile networks aims to ensure privacy by flooding user interests with dummy interests and avoid a trusted server that participates in each interest matching process.

III) Literature Survey:

Narrowing the safety challenges & solutions techniques down from OPP nets & delay tolerant networks to MSNs.[1]

Privacy Preservation matchmaking protocol for mobile social networks that lets a potentially malicious user learn only interests that he has common with a nearby user, but no other interests.[2]

Different architecture of the MSN are presented & each supports different data delivering scenarios.[3]

Unique characteristics of social relationship in MSN give rise to different protocol design issues. These issues & related approaches to address data delivery in MSN are described.[3]

Approaches utilizing rust assumption on TTP (Trusted Third Party) for security.[6]

MobiClique successfully builds & maintains an ad hoc social network leveraging contact opportunities between friends & people sharing interests for context exchanges. [4] proposed a system which is an innovative congestion control algorithm named FAQ-MAST TCP (Fast Active Queue Management Stability Transmission Control Protocol) is aimed for high-speed long-latency networks. Four major difficulties in FAQ-MAST TCP are highlighted at both packet and flow levels. The architecture and characterization of equilibrium and stability properties of FAQ-MAST TCP are discussed.

Privacy Preserving "used connections" services in which the service provider is untrusted and users are not assured to have pre-established social relationships with each other.[5]

Short range wireless communication & standard cryptographic practices to mimic the behavior of user in existing missed connections serious such as Craigslist.[5]

Private processing decentralized social networks where each user could maintain, store and distribute his/her data to his/her friends.[8]

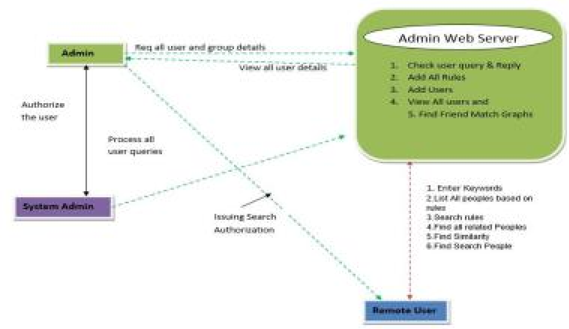
IV) Analysis of reference:

A thorough analysis of reference papers has revealed a tendency to focus on improved usability in contrast to security.

- Secret information is not secure and can be accessed by malicious user.
- Sybil attacks, that forges the data in the networks, are common.
- False identities can be used to steal the data.

Furthermore, mobile social networking is a pervasive communication platform where users can search over the interests and query neighboring peers to obtain the desired information. As such many security and privacy issues arise which need to be effectively addressed. Though lots and lots of solutions are present which help in providing secure encryption, no such all-prevailing mechanism exists which helps in obscuring the entire process. A great deal of work has been done to provide solutions for improved social networking but secured interest sharing without the use of trusted third-party (TTP) or secure server has oftentimes remain ignored and forgotten.

V) Architecture Diagram:



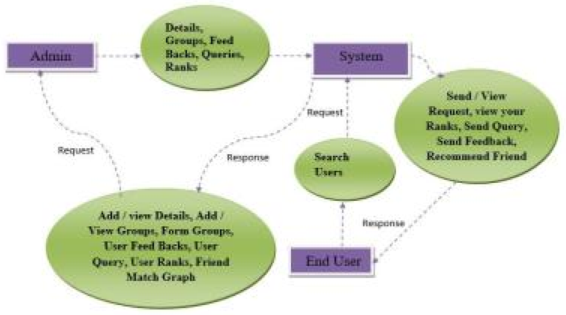
Remote User: The remote user present in the mobile network can search for the interests among like-minded people.

Web Admin: Reporting for all incoming requests and forwards information to the admin.

Admin: The admin checks the security credentials of the user by forwarding the requests to system admin. After verification of user identify, it forwards the request back to the web admin where the privacy mechanism and randomized-QBE algorithm is initiated.

System Admin: The system admin authenticates user credentials and gives the go-ahead for processing all user queries.

VI) Data Flow Diagram:

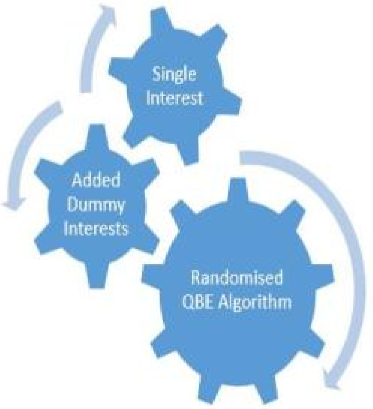

Admin
Details, Groups, Feed Backs, Queries, Ranks
System
Send / View Request, view your Ranks, Send Query, Send Feedback, Recommend Friend
Request
Request
Response
Search Users
Response
Add / view Details, Add / View Groups, Form Groups, User Feed Backs, User Query, User Ranks, Friend Match Graph
End User

VII) Algorithm:

- Diffie-Hellman key exchange has the end to end protocol used.
- Addition of dummies to increase ambiguities.
- START
- Using appropriate prime number combination produce relevant Diffie-Hellman key.
- Flood system with dummy interests using randomized QBE algorithm.
- Increase payload overhead.
- Decipher key for secure end to end communication.

The proposed Random-QBE algorithm provides personalized anonymity in user collaboration algorithm and preserves both query and location privacy. The insertion of algorithm mechanism over real-time data could achieve objectives effectively. The algorithm obfuscates query and location data by hiding the real query and location behind dummies and collaborative users.

The data flow diagram shows the graphical representation of the data through the system mechanism and provides an overview of the information model. The End user is involved in the searching of users based on interests; the user can also view details, form groups, formulate queries and perform other various tasks. The job of providing security through the randomized-QBE algorithms falls on the Admin; which can to authorize and validate users.



Furthermore after assimilation of the real-time interests with dummy interests, the appropriate decision tree has been formulated by utilizing an improved version of C4.5, the EC4.5. It improves on C4.5 by adopting the best among three strategies for computing information of gain continuous attributes.

The first strategy computes the local threshold using the algorithm of C4.5, which in particular sorts cases by means of the quick sort method. The second strategy also uses the algorithm of C4.5, but adopts a counting sort method. The third strategy calculates the local threshold using a main memory version of the Rain Forest algorithm, which does not need sorting. The selection of the strategy to adopt is performed accordingly to an analytic comparison of their efficiency.

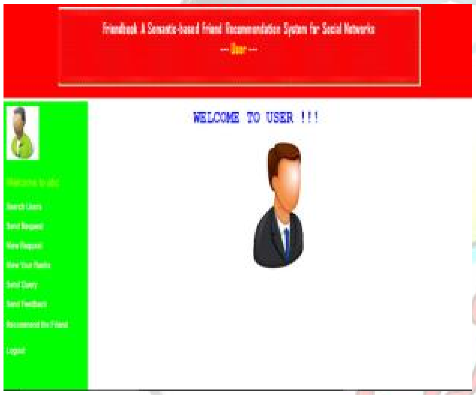
VIII) Module Description:

A Users

In user's module, the admin can view the list of users and list of mobile users. Mobile user means android application users.

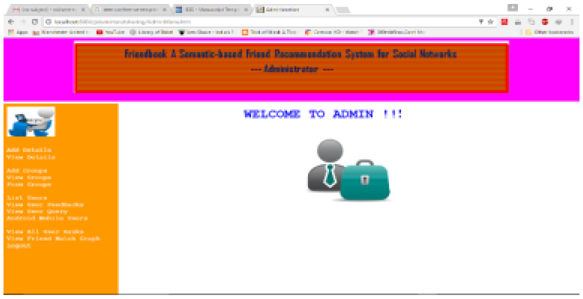
A.1. User

In this module, there are n numbers of users are present. User should register before doing some operations. And register user details are stored in admin module. After registration successful he has to login by using authorized user name and password. Login successful he will do some operations like search users, send friend request, view your rank, send query, send feedback, Recommend the friend and logout.



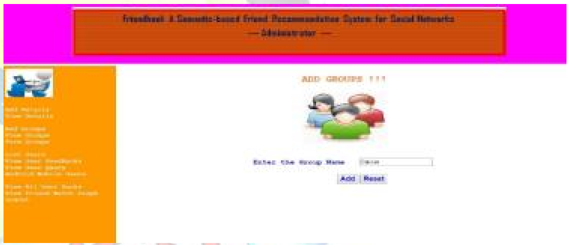
A.2. Admin

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as add details, view details, add groups, view groups, from group, list of users, view user feedback, view user query, Android mobile users, view all user ranks, view friend match graph and logout. The admin can view the registered users, and also admin can view the user feedback, view user query, and also view the android application users.



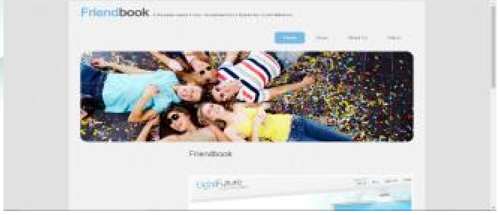
B Add Groups

In this module, the admin can add number of groups. After adding a group admin can view the all groups, and also admin can add user to particular group, after adding successful he will get a response from the server.


Friendbook A Semantic-based Friend Recommendation System for Social Networks
--- Administrator ---
ADD GROUPS !!!
Enter the Group Name
Add
Reset

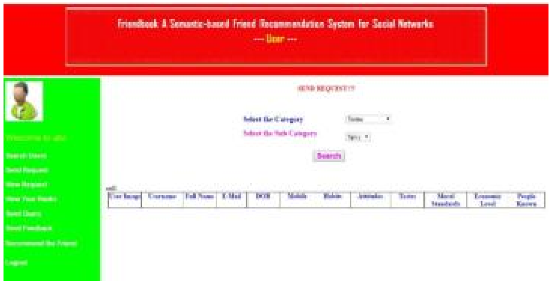
C View friend match graph

In this module, the admin can view the matching friends. If the admin click on view friend match graph button, then all user matching graph will display with their tags such as habit graph, attitude graph, tastes graph, moral standard graph and economic level graph with all user names.



D Send Request

In this module, the user can send friend request to another user. If the user clicks on send request button, then the friend request will send to particular user. And also user can view the all request. After accepting the request response will send to user. And also user rank will be increased based on the friends.



FriendBook A Semantic-based Friend Recommendation System for Social Networks
--- User ---

SEND REQUEST!!

Select the Category
Select the Sub Category
Search

User Image	Username	Full Name	E-Mail	DOB	Mobile	Habits	Attitudes	Tastes	Moral Standards	Economic Level	People Known

IX) Conclusion:

The pervasiveness of interest and location sharing in mobile networks raises increasing privacy concerns. The proposed mechanism mainly applies an improved Randomized Query Block Exchange Algorithm to flood the user interest data and make it more secure. The foundation of this algorithm lies in the prevalent dependency on secure or third-party server. Other improvements that will help increase both service timelines and prolonged hop-distances for communication can be added in future systems.

X) References:

[1] Yashar Najaflou, Behrouz Jedari, Feng Xia, LT Yang & MS Obaidat, "Safety challenges & solutions in mobile social networks", IEEE Syst J., vol. 9, no. 3, pp. 834-854, Sep. 2013.

[2] Q. Xie and U. Hengartner, "Privacy-preserving matchmaking for mobile social networking secure against malicious users", in Proc. IEEE 9th Int. Conf. Privacy Secur. Trust(PST), Jul 2011, pp. 252-259.

[3] N. Kayastha, D. Nujate, P. Wang & E. Hossain, "Application, architecture, & protocol design issues for mobile social networks : A survey", Proc IEEE, vol 99, no 12, pp.2130-2158, Dec. 2011.

[4] Christo Ananth, S.Esakki Rajavel, I.AnnaDurai, A.Mydeen@SyedAli, C.Sudalai@UtchiMahali, M.Ruban Kingston, "FAQ-MAST TCP for Secure Download", International Journal of Communication and Computer Technologies (IJCCTS), Volume 02 – No.13 Issue: 01 , Mar 2014, pp 78-85

[5] J. Manwweiler, R Scudellari & L.P. cosc, "SMILE : Encounter-based trust for mobile social services", in Proc 16th ACM conf. comput. Commun. security (CCS), 2009, pp. 246-255.

[6] Fizza Abbas, Obaidullah Rajput, Heekuck OH, "PRISM: Privacy Aware Interest Sharing & Matching in Mobile Networks", Proc. IEEE, vol. 4, pp. 2594-2603, May 2016.

[7] Fenghua Li, Hanyi Wang, Ban Nui & Hui Li, "A practical Group Matching Scheme for Privacy Users in Mobile Social Networks" Proc. IEEE Wireless Communication & Networking conference (WCNC-2016) Track-3 Mobile & Wireless N/w s, 2016.

[8] Eric Klukovich, Esra Erdin & Mehmet Hadi Gunes, "POSN: A Privacy Preseving Decentralized Social N/w Appn for Mobile Devices", in Proc. IEEE /ACM ASONAM 2016, Aug. 2016, pp. 1426-1429.