International Journal of Advance Research in Science and Engineering
Volume No.08, Issue No.03, March 2019
www.ijarse.com
IJARSE
ISSN: 2319-8354

PRISM: PRIVACY PROTECTION IN SOCIAL NETWORKS USING INTEREST SHARING AND PATTERN MATCHING METHOD

Mr.M.Saravanan (AP/CSE), S.Jayashree, S.Kalishwari, B.Malathi

Department of Computer Science and Engineering,
Mahendra Engineering College for Women (India)

ABSTRACT

Social Network services uses profile matching to help user find friends with similar attributes such as interest, location, background, etc. However, privacy concerns often hinder users from enabling this Functionality. In social network, users face the risk of hacking, leaking or expose of their personal information & location Privacy. The proposed model, Privacy Aware Interest Sharing & Matching Protocol allows users to match their interest with other without reveal their real interest & Profile & vice versa. Therefore, mutual interests need to be found in a privacy preserving manner. PRISM enables users to discover mutual interests without revealing their interests. Unlike existing approaches, PRISM does not require revealing the interests to a trusted server. Moreover, the protocol considers attacking scenarios that have not been addressed previously and provides an efficient solution. The inherent mechanism reveals any cheating attempt by a malicious user. To limit the risk of privacy exposure, only minimum information about interest attribute of the users is match with prevention of real profile attributes. It is Secure & almost preventing from hacking profile of users.

INTRODUCTION

Online social network has gained tremendous momentum in the early years due to the increasing of mobile devices like smartphones and tablets as well as pervasive computing availability of network services. So, the technologies like GPS, wireless localization techniques for mobile have made the generation & sharing of real time user location updates available. Location aware mobile social network represent cyber-physical system, which connect mobile devices within local physical proximity by using both smart phones & wireless communication. In Web-based online social networking location-aware mobile social network allow users to have face to face social interaction in public places. Such as airports, trains & Stadiums.

As a result, the issue of privacy on sites like has received significant attention in both the research community and the mainstream media. The goal is to improve the set of privacy controls and defaults, but it is limited by the fact that there has been no in depth study of users' privacy settings on sites. While significant privacy violations and mismatched user expectations are likely to exist, the extent to which such privacy violations occur has yet to be quantified.

International Journal of Advance Research in Science and Engineering
Volume No.08, Issue No.03, March 2019
www.ijarse.com
IJARSE
ISSN: 2319-8354

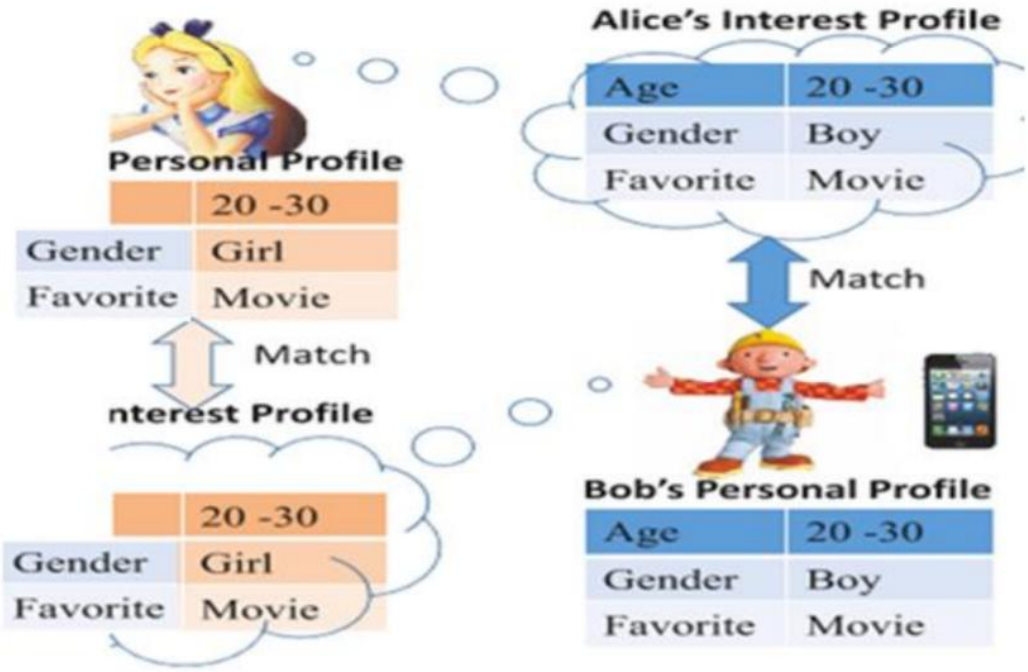

Fig.1

Existing System

Profile matching is important for the wide use of mobile social network. Finding the match able, nearby similar interest is always first prioritize for any social network. The Mobile social network pays limited heed to security & privacy concerns relate with revealing users personal network preferences & friendship information to pervasive computing. In Mobile Social Network, user faces the risk of hacking of their personal information & location privacy.

Disadvantages

- Under these circumstances, attackers can directly associate the personal real profiles with Real user & then do more attacks.
- Loss of privacy can expose users to unwanted spams, scams, cause social reputation, damage, and make the victims of blackmail.

Proposed System

To prevent these all issues of hacking, leaking & damage we introduce the protocol for it. So, that securely matches the private information of two users. The main objective is to improve the existing matchmaking protocols & help users to securely perform matchmaking without revealing unnecessary data.

Advantages

The system carries four major tasks.

- Protocol provides a secure & privacy preserving in order to find mutual interest of user.
- Provide effective means to prevent from hammering to user's profile.
- These include attacks during matchmaking & interest revealing.
- Provide protection against Sybil attacks by limiting user by at most one device.

Modules

The project has been divided into five modules:

1. Social Member Module
2. Identity Verifier Module
3. Match Making Module
4. Interest Revealing Module
5. Graph Report Module

Social Member Module

In this module, new users are allowed to register their details. After that the user will get the access permission for login their details through a login. Users can access their account through they logged in. The Login Module is that allows users to enter a User Name and Password to log in. This module can be placed on any Module Tab to allow users to login to the application. After successful login, user account will be redirected to the home page. Here the user can update the profile with more information. This updating can help the other users to select he/she has a friend.

Identity Verifier Module

Initial setup phase contains the initialization of all requests from users. It first initiates a request with identity verifier (IV) and identity verifier verifies the request and generates a unique id, then it provide unique IDs (UID) to the user. With the help of unique id (UID) user only can login to their system.

Match Making Module

After completion of initial setup phase the matchmaking phase is used to matches the user's interest.

Following step shows matchmaking phases working.

User1 prepares a matchmaking request that includes her exponentiated interests, and sends his/her request to user2. User2 view the details of user1 and profile mating then he/she accepts are declining the request. If user1 accept the request they can easily exchanging these messages. If user2 decline the request there was no further communication with those peoples.

Interest Revealing Module

User1 and user2 exchange their matched interests in order to make it sure that both parties have exactly same matches. User1 and user2 must have exactly same and equal number of matches. Either they do not have any matched interests or they must have equal number of matches with same interest values. Let p be the number of matched interests at user1 side and q be the number of matched interests at user2 side.

As mentioned above, P and q are matched interests at both sides and if there is no cheating then p and q must match exactly. It is interesting to note that both user1 and user2 do not know others matched values. All they know is their calculated values (p in case of user1 and q in case of user2). Being honest assures user1 as well as user2 that the other value should be same as theirs. User1 generates a random secret n1, concatenates her interests that are matched with Bob in alphabetical order, and sends it to user2 as a commitment.

International Journal of Advance Research in Science and Engineering
Volume No.08, Issue No.03, March 2019
www.ijarse.com
IJARSE
ISSN: 2319-8354

Similarly, user2 generates n2, computes and sends this to user1. Next both parties exchange n1 & n2 and find hash value of a & b. Both parties check whether h (A i) == h (B i). If yes, the matchmaking is successful, else the victim sends the protocol recordings to IdV.

Graph Report Module

In this module, The profile matching will shown to the particular matched two users after getting the profile match rating he/she can approach to be as a friend.

The profile matching is calculated by three basis Personal, Basic and Life Style. The graph shows the Personal rating are based on the Qualification, Native and so on.

The Basic rating is calculated by the basic needs the require to be as a friend like mother tongue, Marital Status, Working Palace and so on.

And finally the lifestyle rating is calculated by their favourites like favourite movies, favourite colour, favourite music, music Director, Actor, Actress and the food habits.

SYSTEM ARCHITECTURE

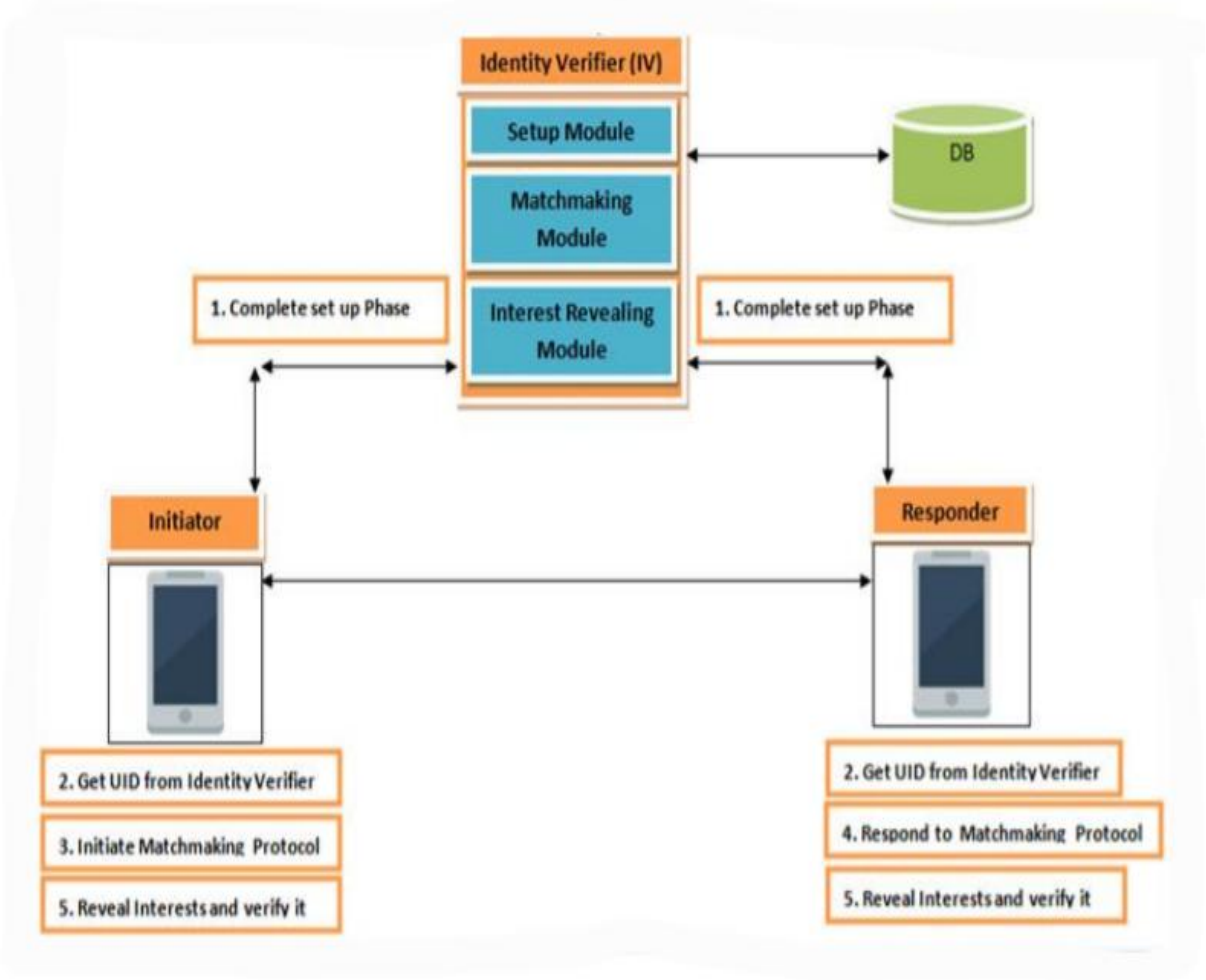

Fig.2

SYSTEM REQUIREMENTS

Hardware Specification

Processor	:	2.4 GHz processor
Main Memory	:	1 GB
Ram	:	1.00GB
Hard Disk	:	240GB
Monitor	:	CRT Monitor 15inch
Keyboard	:	Multimedia Keyboard
Mouse	:	Optical mouse

Software Specification

Operating System	:	Windows 7
Front-End	:	PHP
Web Server	:	Apache
Back End	:	MySQL

CONCLUSION

This proposed model provides efficient privacy protection and interest sharing protocol in mobile social networks. Here provided novel attacks scenarios and their efficient solution. Unlike existing approaches, PRISM does not require a user to reveal interests to a trusted third party and only uses it as an identity verifier and conflict resolver. The proposed use of unique identity for a user helps prevent Sybil attacks. With the help of implementation that shows the feasibility of PRISM. Moreover, with a comprehensive security and complexity analyses, also show the robustness of PRISM against various attacks as well as its efficiency.

BIBLIOGRAPHY

Book Reference

[1] "Beginning PHP and MySQL", W.Jason Gilmore, Apress Publication, Third Edition.

[2] "Learning PHP & MySQL", Michele E.Davis and John A. Phillips, O'Reilly Publication, Second Edition.

[3] "PHP and MySQL Web Development", Luke welling and Laura Thomson, Pearson Education, Fourth Edition.

[4]"Safety challenges and solutions in mobile social networks," IEEE Syst. J., vol. 9,no. 3, pp. 834_854, Sep. 2013.

[5] "A trust lessbroker based protocol to discover friends in proximity based mobile social networks, 'in Information Security Applications. Switzerland: Springer, 2014,pp. 216_227

Website Reference

- www.php.net
- www.wikipedia.com
- www.w3schools.com