Search and Privacy Mechanism for Mobile Social Networks

Vinay Kumar[1], Karan Singh[2], Sushil Kumar[3]

[1]M.Tech Student, School of ICT, Gautam Buddha University, Greater Noida, India
[2]Assistant Professor, School of C&SS, Jawaharlal Nehru University, New Delhi, India
[3] Al FalahSchool of Engineering and Technology, Faridabad, India

Abstract

Mobile social networking applications have become popular very increasingly for communication and interaction, and users' participation has growing tremendously. Currently online social networks provide simple access control mechanisms with selected users to govern only access to information contained in their own spaces. Mobile Social networking applications have become a very popular for communication and interaction, and participation of user has growing tremendously. There are many problems in mobile social networking sites. In this paper, we have proposed a location based search model for easily finding the new friends whose interests are matched with our interest. According to this model, we can interact with new environment and join our favorite activity online and also interact with that activity members, also provide the present location of users.

Key Words: *Social network, Mobile computing, Mobile privacy, Location based search model.*

1. INTRODUCTION

In social networking sites, other than communicating with existing friends, people can find and make friends with other people with similar interests or from the same school or company etc. Mobile social networking (MSN) services to connect to their social communities with a mobile device, through one or more available mobile channels. Members share experiences, interests, opinions, presence information and personal content through their mobile devices. Mobile adds new capabilities to social networking, such as location-related services and new visualization mechanisms. A current trend for social networking websites, such as Facebookis to create mobile apps to give their users instant and real-time access from their device. Some person share their personal idea and information with friends.

1.1USE OF MSNs-

1) Users share their ideas in social mobile network by the help of smart phone.

2) The main focus of mobile social networks is on mobile use like mobile communication, location-based services, and augmented reality, requiring mobile devices and technology.

Mobile social networking integrates these two fast-growing services together. People walk around with their mobile devices and meet different people, known and unknown ones, every day. Mobile social networking applications take advantage of the mobility of the mobile devices.

Mobile social networking integrates these two fast-growing services together. People walk around with their mobile devices and meet different people, known and unknown ones, every day. Mobile social networking applications take advantage of the mobility of the mobile devices and design systems for users to meet potential friends with similar interests or some other criteria. When two mobile devices are physically located close, they could start to exchange information without human interaction.

At the same time mobile phones are becoming more powerful and increasingly offer high speed Internet connectivity. Because of this people expect these social networking services to be available on their mobile device Mobile systems research is often done using ordinary smartphones. All major smartphone platforms, Android, BlackBerry, iPhone, Symbian and Windows Mobile, support development of third party applications [13]. Each platform provides its own approaches to application development and application level resource management.

A. Mobile Computing

Mobile computing is called the portable and small computers, which have Personal Digital Assistants (PDA) like as mobile phones, laptops and palmtops etc. In this growing technological world, People are habitual to work o computer and internet. These two has become the most important part of life. Today every people want mobile devices because of their features and it works like a computer. It has also kept the data like a computer.

B. Social Networks

A social networking service is an online service, platform, or site that focuses on facilitating the building of social networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centred service whereas online community services are group-centred. Social networking sites allow users to share ideas, activities, events, and interests within their individual networks.

Social networking is the grouping of individuals into specific groups, like small rural communities or a neighbourhood subdivision, if you will. Although social networking is possible in person, especially in the workplace, universities, and high schools, it is most popular online. This is because unlike most high schools, colleges, or workplaces, the internet is filled with millions of individuals who are looking to meet other people, to gather and share first-hand information and experiences about cooking, golfing, gardening, developing friendships professional alliances, finding employment, business-to-business marketing and even groups sharing information about baking cookies to the Thrive Movement.

C. Existing Mobile Social Network Applications

MSN users [7] constantly search for ways to interact, engage, and share information while on the move through mobile devices (such as smart phones and tablets). Some newer devices support fourth-generation communication technologies, motivating vendors to provide services on a range of platforms, including Android, BlackBerry, OS, and Windows 8. In addition to hardware improvement, application developers are moving toward mobile advertising, TV, and social gaming, as well as toward new services (such as mobile wallets), mobile commerce, and cloud-based services. These services are enticing research topics. Many researchers have tackled these issues.

Here in this study we have tried to provide the solution by location based search model. This is the searching process, through this users will able to search their interested group activities like cricket, news, football and all that in a unknown environment. Through this users interact with new environment and join our favorite activity online and also interact with that activity members, also provide the present location of users.

1.2 SECURITY PROBLEMS

The general problems of securities are discussed as follows.

Mobile Privacy Issues:

Smart phones and other mobiles are just like mini computers. They all have the power and functionality of computers. Our mobiles contain large amount of personal information like contact numbers, photos, videos. Security or privacy [8] risks are inherent to the internet. Our personal information are become the target of malware and spyware. Mobile devices contain the user information that are not usually found on personal computer as telephone calls, text messages, and history of our location.

Other challenge is the devices, small screens, which makes the effective communication. But users have no many options for privacy. Today the application economy is thriving. Mobile app is a development stage, in which developers are focusing on getting new products to market quickly as possible.

Many mobile applications didn't provide the privacy of users. This represents not just a failure, but it is also suggest a lack of attention to application privacy.

2 BACKGROUND & RELATED WORK

Muyuan Li et al. [1] have discussed about the mobile user, that mobile users may face the risks of leaking their personal information and their location privacy. Propose is profile matching protocol, which enables one party to match its interest with the profile of another, without revealing its real interest and profile and vice versa. Authors have used blind transformation algorithm for easily finding the match profile. They have secured from many attacks as profile Leaking Attack, Runaway Attack.

R. Wallbridge et al. [3] have different privacy issues on online social networking sites and they said that when user create their profile once friends a small link connect their profile by photo, video, messenger and comment with each user profile by editing comments and sending messages. Authors have focused on the negative aspects of online social networking sites and control of personal information because

when user place their information on public domain user can easily lose control over the data who sees if and who may use it.

SörenPreibusch et al. [4] have explored the dual nature of friendship relations as an enabler but also as a pitfall for privacy in social networks. Authors have motivated the need for both public and private friend relationships in social networks and explain why maintaining public and private friend relationships in a centralized architecture is easier than in a peer-to-peer one. Friendship is the most fundamental relation in a social network. It is a relation between two members of the network and carries the understanding of friendship from the world. In a social network with a centralized authority and clients being constantly able to establish a connection to this authority, hidden friendships can easily be implemented by views on a user's list of friends. A customized view on the outgoing friendship relations of a SN member is generated for each request. Our approach of securely hashing identifiers for hidden friendship relationships presents several theoretical and technical advantages which are particularly valuable for deployment in mobile social networking:

S Leitch et al. [5] have discussed about the real life security issues and throats with facebook. They have discussed different type of facebook security issues as privacy and confidentially, authentication and identity theft, intellectual property theft vandalism, harassment & stalking, data motion &disparagement, spam and cyber squatting. There all risks are greatest for facebook because fact is that people trust their facebook friends means that identity theft is greater.

Ming Li, el al. [2] have proposed Find U, a set of privacy-preserving profile matching schemes for proximity-based mobile social networks. In Find U, an initiating user can find from a group of users the one whose profile best matches with his/her. And has also proposed novel protocols that realize each of the user privacy levels, which can also be personalized by the users. Author has defined problem of the system model, Adversary Model, Design Goals, then solve the problem. Find the friends to use same protocol and User discovery the friend and establishment Key to easily find friends.

Balachander Krishnamurthy et al. [6] have described the Mobile Online Social Networks

(MOSN) in our study exhibit some leakage of private information to third parties. In this paper presented taxonomy of ways to study privacy leakage and report on the current status of known leakages a device such as a smart phone could be used to access the mobile or full web site via a mobile browser as well as a device-specific application tailored for a MOSN. They have to be aware of the duration of any privacy setting they have made. When they allow some information, such as location, to be used by the MOSN for a legitimate purpose, they have to be aware that it might be handed over to third-parties. They have used the following criteria of inclusion of candidate MOSNs for our study.

RachaAjami et al. [9] have surveyed that everyone are focusing on protecting user's information but they have failed to cover other important issues. For example, User have control over their data and what other can reveal about them but encryption of image is still not achieved properly. Authors have discussed about the Social Network Services and communication interface that are used to establish Social Network relationship between user who have same interests and activities. In this survey authors have highlight some issues related to the security of social networking sites. And discussed the approaches that flip in achieving acceptable levels of security for the social network providers and users.

WaadAssaad, and Jorge Marx Gómez [10] have discussed about the social networking sites that with the growth of social media and software, social networks are forcing companies to increase the activities in their CRM system and social networking sites are a good approach for companies and customers to improve their commutation. Authors have discussed technique to find how social networking software can be used to improve the marketing and to survey how social networking software can be used effectively in enterprises.

NahierAldhafferi et al. [11] discussed about the protection of online social network providers have developed various technique to decrease the threats and risks. There risks include the misuse of personal information which leads to the illegal acts. Here authors objective is to measure the awareness of user on protecting their personal information. Authors have surveyed and get the results to showing the high percentage of the use of smart phones for web services but current privacy settings for online social network needs to be improved to support different type of mobile phone screens. Because maximum number of users use mobile phones for internet service. According to their survey study can be used to develop a new privacy system which will help user control their personal information. Authors have controlled privacy settings from different types of internet mobile phone and supporting various screen sizes.

AmreShakimov et al. [12] have presented vis-à-vis prototype decentralized framework for OSN based on privacy preserving notation of a virtual individual serves. In vis-à-vis user stores their data on their own vis, which attributes access to that data by other. Authors have focused on presenting the privacy on location information. Vis-à-vis use distributed location trees to provide efficient and sealable operation for sharing location information on social groups. Authors have also deployed a vis-à-vis prototype in amazon and measured its performance against a centralized implementation of the same OSN operation.

Noora Al Mutawa et al. [13] have discussed on conducting forensic analysis on three social networking application on smartphones, facebook, tiwitter and myspace. Test has conduct on three smartphones, Blackberrys, iphone, android phone after installing the social networking application on each device. Here authors aimed whether activities conducted through these application were stored on the devise internal memory and focused the location of that data from the logical image of each device. Result has seen that no traces recovered from Black Berry phones. However, iphone and android phones have stored a significant amount of valuable data cut is revered by investigators.

Jingwei Li et al. [14] have made a further treatment on privacy- preserving location sharing in mobile online social networking and have purposed a security improved mechanism namely mobishare is secure in terms of location privacy and social network privacy. Authors have compared mobishare employs dummy queries and private set interaction protocol between the location service and OSN service provider, and provide the full protection of social network against the location service provider mobishare mechanism is used to enable flexible location sharing between both trusted social relations and untrusted strangers.

Wei Wei et al. [15] have presented mobishare it is a system that provides flexible privacy preserving location sharing in MOSN. And support a variety of location based application, mobishare is also enables location sharing between trusted and untrusted strangers. In mobishare, neither the social network servers nor the location has the complete knowledge of user's identities and locations. Authors have protected user's location by the malicious users, malicious users are not able to leak the user's information because they are not authorized to access their locations.

Wei Dong et al. [16] have discussed about the increasing popularity of mobile social network and author have developed novel techniques and protocols to compute social issues between two user to discover potential friends. This is an essential task for mobile social networks. They have made three major contributions first they have identified the range of potential attacks by analyzing real traces. Second, also developed a novel solution for secure proximity estimation. Third, they have demonstrated the feasibility and effective of our approaches using real implementation on smartphones. And proof it is efficient in both computation time and power consumption.

Mulliner, C [17] have discussed about the privacy problem with the mobile phone because today everybody can afford mobile phone and access the internet on it. Almost every mobile have an integrated web browser user use that and accessing the World Wide Web. Author has investigated possible privacy problem of mobile phone web access. They have also determined that worldwide privacy problem occur when accessing the www from mobile phone. According to they have seen that what kind of data is leaked and leaks it. Privacy leakage is related the HTTP proxies that is operated by mobile phone. These proxies inject additional headers into HTTP connections and become the cause of privacy leak.

Wenbo et al. [18] have used four square as an example to introduction location cheating attack, which easily pass the current location verification mechanism. Authors have also crawl the foursquare website. After analyzing the crawled data, they have seen that automated large scale cheating is possible. Authors have crawled two types of information. User's profiles and venue's profile from foursquare website. After that they has demonstrated that their attacking approach works as expected and location cheating is really harmful for the development and deployment of location- based deployment of location-based mobile social network services.

Nan Li and Guanling Chen [19] have discussed that location based mobile social network are becoming very popular. They have presented a multi layered friendship model for location based MSNs, and compare this model with data mining algorithm, found that the multi layered model provide better performance, especially in top rank predictions. In this model, authors have attached each update with user's location. Authors have collect user's profiles and their friend lists and then built three layered friendship model to correlate the relationship between user's friend connections with their profiles.

JulienFreudiger et al. [20] have discussed about online social networks because it is becoming popular and allowing mobile users to share their location with their friends. Users share their location on social networks, and third party can easily learn the user's location from localization and local visualization services. To protect your's location privacy, authors have designed and implemented a platform independent for users to share their location on online social networks. They have used encryption technique to protect user's location.

Okoro et al. [21] has introduced that user participation on online social network has increased tremendously. The types of data uploaded and shared on user profiles also include sensitive information. In this paper, highlights the potential attacks owing to the vast amount of user personal information available on social networks. And proposed a theoretical model for resolving the problems associated with the current default privacy and wider accessibility design implemented by most social networks. This paper has also discussed the prevailing attacks on social network users.

Ping Zhang et al. [22] have proposed a trust framework for social networks, including defining new trust metrics and their combinations, which capture both human trust level and its uncertainty, while being intuitive and user friendly. They have also proposed several security mechanisms, including filtering information on social networks and increasing the efficiency of advertisement and influence on social networks.

They have also summarize the trust evaluation arithmetic based on error propagation theory, using trust metric and how to adapt them to comply with psychological implications. There are two basic types of trust prorogation operations: trust transitivity and trust aggregation.They introduced two trust metrics: impression and confidence that on one hand are intuitive and on the other, are similar to measured value and its error used in measurement theory.

Vorakulpipat et al. [23] have discussed about the social networking websites because these are using tremendously. many people are not properly aware of the risk with using these websites and applications and examines the issues of security, privacy and trust in online social networking sites with using viewpoints. So, Authors have considered two countries like Thailand and UAE both countries have witnessed of using social networking sites. They have three instruments like survey question interviews are use to better understanding the result. After survey of two countries, they said especially women are felt more comfortable using social networking sites.

Potdar et al. [24] that Social networking is used in and outside every organization. There are many social networking whites as sites as facebook, twitter, orkutetc and issues in different way as chatting, messaging, games, video, photo upload etc. however, everybody observed that these are many user face different problems as identity theft stealing of personal information. Authors have discussed on various kinds of security issues authors main focused is on the many issues of security and also dual with possible solutions on issues. User said that almost 25.61% users of social networking wed sites are number aware of the security issues.

Joshi et al. [25] have proposed a small survey about the online social network. In this survey, authors have focused on the privacy aspect and their concerned on the possible attacks. Because users share their data on social networks without bring aware of consequences. Every users profile contains the sensitive information and users as advertisement. So, attackers can take the advantage of it. Authors have discussed a preserving privacy in social network data and identity a privacy attacks as neighborhood attacks by mathematical formulation and computational models for security and privacy.

Keister et al. [26] have proposed new security architecture called socially keyed (sokey) architecture achieving zero possibility for personal information leak from Social networking sites. This architecture is very confidential to make sure that providing information on social networking sites will never leak.

Gharibi et al. [27] have discussed about cyber threat. Cyber threat may be unintentional and intentional and social networking site are not for communication and interaction with other people but also a effective way for business promotion. Authors have investigate cyber threat in online social networking sites cyber criminals captures the users data then transferred to the attackers and terrorist and adults predators, mostly facebook is used for crime because every user share their information on facebook account from that criminals pick up users data and used on adult websites.

Wallbridge[28] have different privacy issues on online social networking sites and they said the when user create their profile once friends a small link connect their profile by photo, video, messenger and comment with each user profile by editing comments and sending messages. Main focused of this paper on the negative aspects of online social networking sites and control of personal information because when user place their information on public domain user can easily lose control over the data who sees if and who may use it.

Kumar et al. [29] have proposed a architecture for securing the information between user and a secures request response architecture, because social networking is the easiest way for communication. Social networks contains the millions of user each user have their own profile that contain more information. Users share so much data on social networking sites and this action became the target of attacks. Attackers found the very easy way to steal the information through these networking sites.

S Leitch and M Warren [30] have discussed about the real life security issues and threats with facebook. They have discussed different type of facebook security issues as privacy and confidentially, authentication and identity theft, intellectual property theft vandalism, harassment & stalking, data motion & disparagement, spam and cyber squatting. There all risks are greatest issues for facebook because fact is that people trust their facebook friends means that identity theft is greater.

Justin Becker and Hao Chen [31] have proposed a privAware tool to detect unintended information loss in online social networks to identify privacy risk and provide solution to reduce information loss because measuring the privacy risk in online social networks is a big challenge. Millions of users are participating in social networking sites and share the data in a huge large amount.

Isfahan and Iran [32] have introduced profile cloning and identity theft attacks. Fake profiles are the clone profiles. They have discussed only two type of clone profile as profile cloning. Users create same fake profile in ONS that have nature. Authors have produced a framework for detecting profile cloning in ONS. The detection framework is used for detecting the fake profile. In identity clone attack an user adds victims friend in the clone profile. We can say that by using detecting framework approach clone profile can be detected more accurate.

3. LOCATION BASED SEARCH AND PRIVACY SOLUTION

We have tried to provide the solution by location based search model. This is the searching process, through this users will able to search their interested group activities like cricket, news, football and all that in a unknown environment.

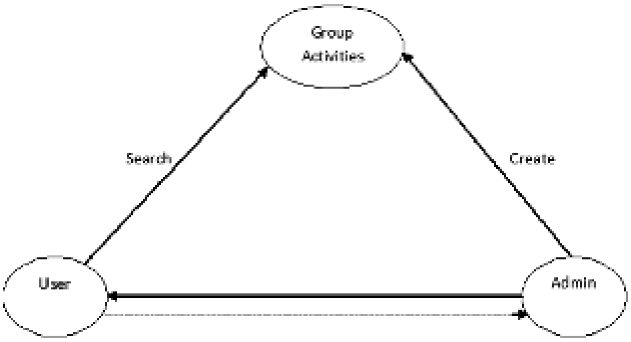


Fig-1: Activity search model

In Figure1. Admin creates group activities, and there different- different admin of different- different place. For example: A user goes to different place and wants to join his interested activity like cricket. Then he will search that activity, user connects to the admin through the location server. Because location server connects this user to the new environment and show user's interested activity nearby of that environment. After getting his interested group activity, user will automatically connect to admin of that group. But they both are not able to permit to see all information of each other. Admin will see only user's name and profession. And user will see only related information of group activities. User will not interact to admin's profile.

There is no direct interaction between user and admin, they both are connect through the activity groups. According to this model, we can easily interact with a new environment.

4. LOCATION BASED SEARCH PSEUDO CODE ALGORITHM

This algorithm is proposed for providing the exact current interested location. In this we have tried to provide better privacy with this friendly environment. This is very friendly for every user and easy to understandable.

```
Input
k as keyword or sentence
            L as location
Output
gas group with location
Search function (k, l)
str1            k
str2            l
temp                    k temp is array, store sentence
which in split by blank space
str3sql query with array values and location
con             create connection with database
pst             pass query with con and str3.
rst             execute query with pst.
res             fetch value from rst
return res;
end function;
```

5. LOCATION BASED SEARCH PROCESS

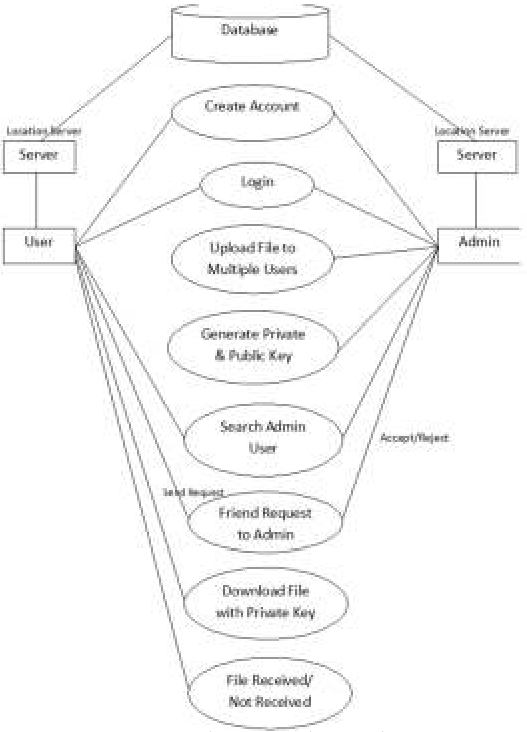


Fig-2: Location Based Search Process

This model is a process of system. In figure 2.admin creates a account and location of admin is held on server, The all information related to the admin is kept on database. Location on the server of the admin will be changed according to the admin. And then a user is also createa account user and admin both are log in their account. Admin upload a file on his account to multiple user. Admin also generate the public and private key. If user is on a new place than server will search current location of user and user wants to join activity group of his nearby. User searches his interest group and easily finds the group. If admin of that area has already created that group and after that user will send the friend request to admin to joining that group. Then admin will check the user's profile than accept otherwise reject. If admin accept the request of user download the file from admin's profile with private key but related to that activity. And if admin rejects the request of user. According to this model user can easily find the new friends whose are matched with user's interest. This will be used especially for saving the time and through this user can easily interact with new environment. After meetings, users will increase their social network. In this main thing is that user only goes inside the group activity not in admin's profile. Information of admin will be kept safely on the database.

The procedure for proposed work is as follows.

1. Register.
2. Login.
3. Server automatically searches the current location of users.
4. Users search of their interested activities like cricket, gym, hospital, yoga so on..nearest to the current location.
5. Activities are list out in front of user.
6. Users select their interested activity.
7. Send the request to that group (request goes to admin of that activity).
8. Admin verify the details of users like name, age, date of birth and profession only. After that accept or reject.

9. If accept, users add in group.

10. Users can able to see the details about the group and also see group members.

11. Users are permitted only for seeing the group members but not for seeing the profile of any member of that group.

6. SYSTEM MODEL

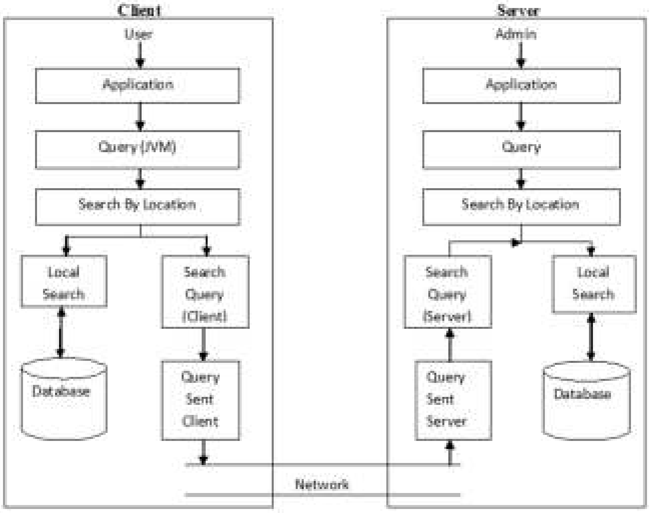


Fig-3: System Model

User: A user is a person who uses a computer or networkservice. A client often has a user account and is identified by a username. It is also include login name.

Application: Application is a platform through which end user works. Application gives a better interface for interacting with a project.

Query: Through the application, we feed the query and Java Virtual Machine (JVM) converts query into the machinery language.

Search By Location: After Converting the query into machinery language search the current location of the user.

Local Search: First of all client search their location on their local database.

Search Query: After searching the query of the client side, query sends to the server side.

7. WORK ON PLATFORM

The proposed work is implemented in JSP [34]. It is one of the goals to make the environment for controlling the data on multicast networks. For this, Windows 8 Operating System was used and in the backend we have used MYSQL database [33] and platform is SQLyog. Netbeans tool is used for implementation of this proposed work. It is an integrated development environment (IDE) for developing primarily with Java, but also with other languages. We have analyzed our proposed work by JMetter tool. This tool is used for testing. Apache JMetter may be used to test performance both on static and dynamic resources [35].

8. RESULTS

A snapshot of main interface of social networking site through this we have done our proposed work as shown in figure 4. Users are search group name according to the current location. And nearest groups of the user current location are listed out. According to this work, users interact to the unknown environment and search their interested activity and join that with suggestion of anybody.

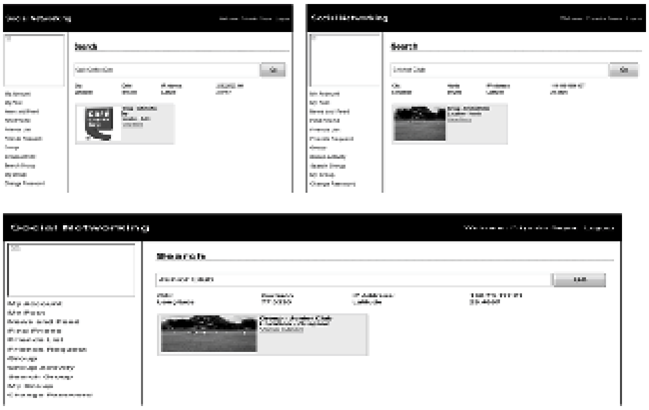


Fig-4: Search Activities

After the seen the group user are send to join group request to the admin as shown in figure 5.

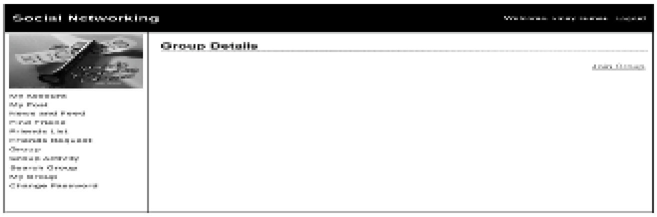
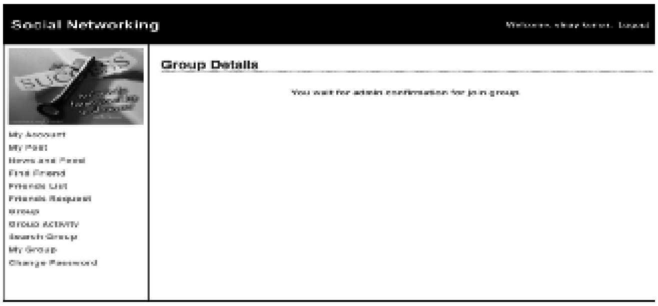


Fig-5: Join Group

After selecting the group user join group sends the confirmation to admin after that admin confirms user's conformation according their eligibility. Without joining the group, user would not able to see the information regarding the group as shown in figure 6.

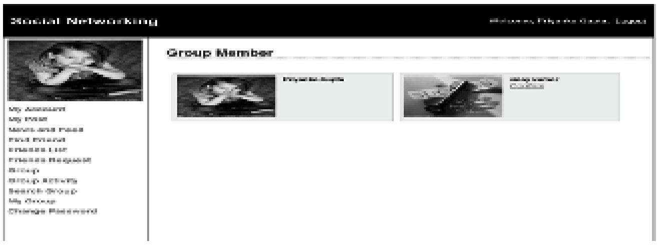


Group Details

You wait for admin confirmation for join group.

Fig-6: Wait for Confirmation

After the sending the joining group request so the admin seen the group request and check to the person and confirm to the request as shown in figure 7.



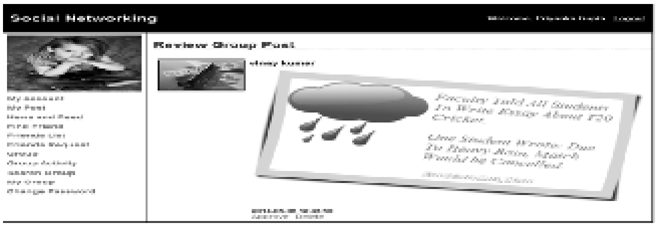
Group Member

Priyanka Gupta

Vinay Kumar

Fig-7: Group Members

If any group member or any group activity shares the data on group regarding the activity so, after posting the data they need the approval by admin as shown in figure 7. Because admin confirms that, data is objectionable or not. After seeing that admin approves that post.



Review Group Post

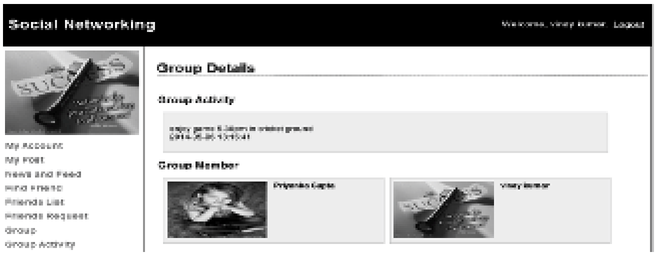
vinay kumar

Faculty told All Students To Write Essay About T20 Cricket

One Student Wrote: Due To Heavy Rain, Match Would be Cancelled

Fig-8: Group Post

If any group member or any group activity shares the data on group regarding the activity so, after posting the data they need the approval by admin as shown in figure 8. Because admin confirms that, data is objectionable or not. After seeing that admin approves that post



Group Details

Group Activity

enjoy game 5.30pm in cricket ground
2014-05-05 13:15:41

Group Member

Priyanka Gupta

Vinay Kumar

Fig-9: Group Details

9. RESULTS ANALYSIS

We have implemented our proposed work. And we have also analysed the effect of throughput and standard deviation. The discussions regarding this dissertation are given below.

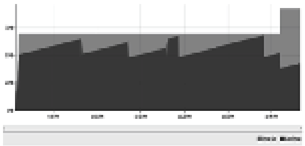


Figure 4.7: Memory (heap)

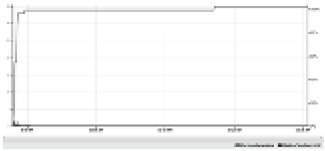


Figure 4.8: Memory (GC)

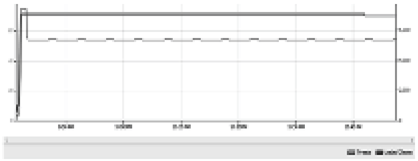


Figure 4.9: Threads/Loaded Classes

In the graph 1, Red shading indicates the allocated size of the JVM server heap. The purple overlay indicates the amount of heap space actually in use. In the example above the allocated heap size at the last update was over 90 megabytes. Of that about 43 megabytes is actually being used to hold Java objects.

The graph 2, Shows two important heap statistics.

- The blue line is the percentage of execution time spent by the JVM server doing garbage collection and is graphed against the y-axis on the right edge of the graph. Time spent by the JVM server doing garbage collection is time that is not available for it to run your application. So if the blue line indicates a large percentage you may want to consider tuning the JVM server by configuring a larger heap size (refer to the -Xmx parameter documentation) or perhaps switching to a different garbage collection algorithm.

- The red line is surviving generations and is graphed against the y-axis scale on the left edge of the graph. The count of surviving generations is the number of different ages of all the Java objects on the JVM server's heap, where "age" is defined as the number of garbage collections that an object has survived. When the value for surviving generations is low it indicates that most of the objects on the heap have been around about the same amount of time. If, however, the value for surviving generations is increasing at a high rate over time then it indicates your application is allocating new objects while maintaining references to many of the older objects it already allocated. If those older objects are in fact no longer needed then your application is wasting (or "leaking") memory.

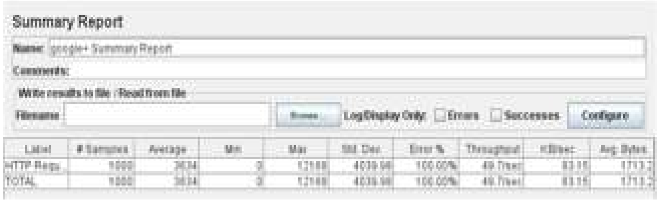
The graph 3, Shows the count of active threads in the JVM.

In this x-axis is showing the number of threads and y-axis is showing the time interval. And red line is the threads and blue line is loaded classes. In this total loaded classes are 78 and threads are 59 according the time interval of running application.

Comparison between Google+ and Proposed Work

In this we have analyzed the two sites as Google+ and proposed work. Through this analysis we can measure the difference Google+ and smedia (proposed work).

Table -1: Google+ Summary Report



Summary Report

Name: google+ Summary Report

Comments:

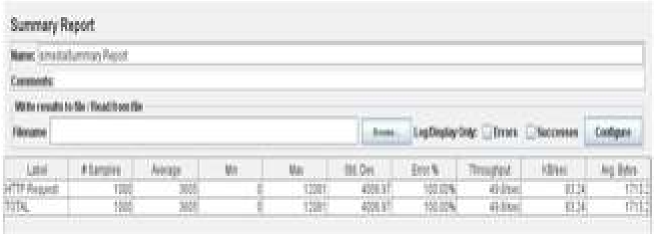
Write results to file / Read from file

Filename: Browse... Log/Display Only: □ Errors □ Successes Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	KB/sec	Avg. Bytes
HTTP Requ...	1000	3634	3	12168	4039.98	100.00%	49.7/sec	83.15	1713.2
TOTAL	1000	3634	3	12168	4039.98	100.00%	49.7/sec	83.15	1713.2

In the facebook summary report we have taken 1000 samples (threads) to test the facebook. This table showing 12168 average load classes at 1000 samples and in this standard deviation is 4039.98, throughput is 49.7 per second. And working time is 83.15 KB per second.

Table -2: Smedia Summary Report (Proposed Work)



Summary Report

Name: smediaSummary Report

Comments:

Write results to file / Read from file

Filename: Browse... Log/Display Only: □ Errors □ Successes Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	KB/sec	Avg. Bytes
HTTP Request	1000	3605	0	12081	4006.97	100.00%	49.8/sec	83.24	1713.2
TOTAL	1000	3605	0	12081	4006.97	100.00%	49.8/sec	83.24	1713.2

In the smedia summary report we have taken same sample like google+ as 1000 samples (threads) to test the smedia. This table 3605 average load classes at 1000 samples and in this standard deviation is 4006.97, throughput is 49.8 per second. And working time is 83.24 KB per second and average bytes are 1713.2.

10. CONCLUSION

We have discussed a solution for easily finding the friends with our interest in the shortest time of duration. In this paper, we have proposed a location based search model for saving our time. Through this, we can direct interact with new friends, and create the connection between new friends. Main thing is that we would have great friend circle. After that, users will able to easily find out their interested activities and create a trusted social network.

In this, server provides the current location of users and location of the users store in the database and then provides the security to users. User's becomes more secure by MSNs. Any other user would not be able to access our account. Because users don't have right to access other user's account. We are done work on system model with the help of location based server for providing the security to the users. We have provided a key through the admin for security purpose.

REFERENCES

[1] Muyuan Li ,HjinZhu, Suguo Du, "Fairness-aware an Privacy-Preserving Friend Matching Protocol in Mobile Social Networks" IEEE, 2012.

[2] Ming Li,Shucheng Yu, Ning Cao, "Privacy-Preserving Distributed Profile Matching InProximity-Based Mobile Social Networks" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 5, MAY 2013.

[3] R. Wallbridge, "How safe is Your Facebook Profile? Privacy issues of online social networks", ANU Undergraduate Research Journal in 2009.

[4] SörenPreibusch, Alastair R. Beresford, "Privacy-Preserving Friendship Relations for Mobile Social Networking" W3C Workshop on the Future of Social Networking, 2008.

[5] S Leitch and M Warren, "Security Issues Challenging Facebook", 7th Australian Information Security Management Conference in 2009.

[6] Balachander Krishnamurthy, Craig E. Wills, "Privacy Leakage in Mobile Online Social Networks " IEEE, 2011.

[7] UN Data accessed nov, 2012.

[8] http://vsual.co/2011/12/indians-use-mobiles-in-a-big-way-infographics/

[9] RachaAjami, Noha Ramadan, Nader Mohamed, and Jameela Al-Jaroodi, "Security Challenges and Approaches in Online Social Networks: A Survey" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.8, August 2011.

[10] WaadAssaad, Jorge Marx Gómez, "Social Network in marketing (Social Media Marketing) Opportunities and Risks" International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT) Vol. 2, No. 1, September 2011.

[11] NahierAldhafferi, Charles Watson and A.S.M Sajeev, "Personal Information Privacy Settings of Online Social Networks And Their Suitability Fof Mobile Internet Devices" International Journal of Security, Privacy and Trust Management (IJSPTM) vol 2, No 2, April 2013.

[12] AmreShakimov, Harold Lim, Ram´onC´aceres, Landon P. Cox, Kevin Li, Dongtao Liu, and Alexander Varshavsky, "Vis-`a-Vis: Privacy-Preserving Online Social Networking via Virtual Individual Servers" 978-1-4244-8953-4/11 in IEEE 2011.

[13] Noora Al Mutawa, Ibrahim Baggili, Andrew Marrington, "Forensic analysis of social networking applications on mobile devices" Digital Investigation 9 (2012) S24–S33.

[14] Jingwei Li, Jin Li, Xiaofeng Chen, Zheli Liu, and ChunfuJiaNankai University, Tianjin, China, "MobiShare+: Security Improved System for Location Sharing in Mobile Online Social Networks" Journal of Internet Services and Information Security (JISIS), volume: 4, number: 1, pp. 25-36, 2013.

[15] Wei Wei, FengyuanXu, Qun Li, "MobiShare: Flexible Privacy-Preserving Location Sharing in Mobile Online Social Networks" INFOCOM, page 2616-2620. IEEE, (2012).

[16] WEI DONG, VACHA DAVE, LILIQIU, YIN ZHANG, "SECURE FRIEND DISCOVERY IN MOBILE SOCIAL NETWORKS" INFOCOM, IEEE, 2011.

[17] MULLINER, C, "PRIVACY LEAKS IN MOBILE PHONE INTERNET ACCESS" 14TH INTERNATIONAL CONFERENCE ON INTELLIGENCE IN NEXT GENERATION NETWORKS (ICIN), VOL.6, 2010.

[18] Wenbo, HeXue and LiuMaiRen, "Location Cheating: A Security Challenge to Location-based Social Network Services" arxiv: 1102.4135v1 [cs.S1] 21 Feb 2011.

[19] Nan Li and Guanling Chen, "Multi-Layered Friendship Modeling for Location-Based Mobile Social Networks" 6th Annual

International on Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous, 2009.

[20] JulienFreudiger , Raoul Neu , Jean-pierreHubaux, “Private Sharing of User Location over Online Social Networks” International Journal of Security, Privacy and Trust Management (IJSPTM) vol 2, No 2, April 2013.

[21] EzinwaOkoro, SteliosSotiriadis, NikBessis, Richard Hill, “Customized Profile Accessibility and Privacy for Users of Social Networks,” Third International Conference on Emerging Intelligent Data and Web Technologies, 2012.

[22] Ping Zhang, ArjanDurresi, YefengRuan, MimozaDurresi, “Trust based Mechanisms for Social Networks,” Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, 2012.

[23] ChaleeVorakulpipat, Adam Marks, YacineRezgui, SiwarukSiwamogsatham, “Security and Privacy Issues in Social Networking Sites from User's Viewpoint”, IEEE Conference in 2011.

[24] BalkrushnaPotdar and Dr. Vilas Nandavadekar, “A Study of Security Issues Faced and Security Measures Practiced by Citizens of Pune City while working on Social Networking Websites”, Tenth International Conference on ICT and Knowledge Engineering in 2012.

[25] Prateek Joshi and C. –C. Jay Kuo, “Security And Privacy In Online Social Networks: A Survey”,IEEE Conference in 2011.

[26] Jacob W. Keister, Hiroshi Fujinoki, Clinton W. Bandy, and Steven R. Lickenbrock, “SoKey: New Security Architecture for Zero-Possibility Private Information Leak in Social Networking Applications”, IEEE Conference in 2011.

[27] WajebGharibi and MahaShaabi, “Cyber Threats In Social Networking Websites”, International Journal of Distributed and Parallel Systems in 2012.

[28] R. Wallbridge, “How safe is Your Facebook Profile? Privacy issues of online social networks”, ANU Undergraduate Research Journal in 2009.

[29] Abhishek Kumar, Subham Kumar Gupta, Animesh Kumar Rai, SapnaSinha, “Social Networking Sites and Their Security Issues”, International Journal of Scientific and Research Publications in 2013.

[30] S Leitch and M Warren, “Security Issues Challenging Facebook”, 7th Australian Information Security Management Conference in 2009.

[31] Justin Becker and Hao Chen, “Measuring Privacy Risk in Online Social Networks”, W2SP in 2009.

[32] Isfahan and Iran, “An approach for detecting profile cloning in online social networks”, 7th International Conference on e-Commerce in Developing Countries in 2013.

"History of MySQL"

[33] . MySQL 5.1 Reference Manual. MySQL AB. Retrieved 26 August 2011.

[34] Severance, Charles (February 2012). "JavaScript: Designing a Language in 10 Days". Computer (IEEE Computer Society) 45 (2): 7–8. doi:10.1109/MC.2012.57. Retrieved 23 March 2013.

"Apache JMeter - User's Manual: Building a Web Test Plan"

[35] . Jmeter.apache.org. Retrieved 2013-09-20.