Secure Multicast Model For Social Networking

Deepa Bharti1, Sandhya Tarar2, Karan Singh3
1 M.Tech Student, School of ICT, Gautam Buddha University, Greater Noida, India
2 Research Associate, School of ICT, Gautam Buddha University, Greater Noida, India
3 Assistant Professor, School of C&SS, Jawaharlal Nehru University, New Delhi, India

Abstract
Social networking applications have become a very popular for communication and interaction, and participation of user 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. Social networking sites allow users to restrict access to distributed data, users; unfortunately, there is no any mechanism to providing the privacy concern over data associated with a group. In this paper, we have proposed and implement a multicasting model for securing the data on group, and we tried to deal with the more comprehensive privacy conflict resolution with the help of this model. This model is used for collaborative management of shared data on online social networking sites. In this we have also provide globally search engine for social networking sites. Through this search engine, users don't need to go to another page and able to search anything on my space.

Key Words: Social networks, multiparty access control, secure multicast networks, process distribution.

1. INTRODUCTION

Social networking sites such as MySpace (over 246 million users), Facebook (over 124 million users), Orkut (over 67 million users), and LinkedIn (over 9 million "professionals") are examples of wildly popular networks used to find and organize contacts. Other social networks such as Flickr, YouTube, and Google Video, are used to share multimedia content, and others such as Live Journal and BlogSpot are used to share blogs [2].

In recent year, we have seen unprecedented growth in Online Social Networking (OSN) sites. We all know that facebook is one of the representative social networking sites claim that it has over 300 million users. To protect user data, access control provide central features or OSN [3].

OSN's such as facebook and google+ etc. are designed to people for share the personal and public information and make social connection with friends, family, and strangers and so on. OSN means of interactions among people in which they create, share, and/or exchange information and ideas in virtual communities and networks. OSN is used to create highly interactive platforms through which individuals and communities share, co-create, discuss, and modify user-generated content [11].

Here this study is proposing a multicast model for providing the better privacy. As social media is used for making good relationship and keep in touch with friends and aware with current environment. But today there are being a problem, our main focus in on facebook that our data on social media is not safe especially on groups. Some members of group misuse data that are posted on group by changing and modification with that data. And now we have been seen in previous studies that there is no better privacy for multicast network for securing our data on social networking sites. In this study, we have tried to stop misuse of social media by the modification with data and we are providing some important privacy options through which group members will always need of admin's permission for doing any type of activity with the data. After that there would no possibilities of any type of modifications. Social media is about expressing opinions freely and we need to maintain that sense of freedom.

1.1 USE OF OSNS

Social Network has the ability to stay in touch with friends and family members from anywhere in the world has millions of people caught up in the excitement of social networking. Because social networks are where the customers are, many enterprises are also turning to social networks as a free and powerful means of communication.

Although OSNs provide access control mechanism for users to govern access to only their information contained in their own space, unfortunately users have no control over data residing outside their space. While each user contains profile information and information may be public or private. So, users don't want to share their information with public.

OSNs provide some space to each user for basic profile and sharing photos and videos with others. When a users distribute their content and photo on a group, every member of group are able see and distribute that. So now these users want more privacy because they don't want to distribute their information.

2. BACKGROUND & RELATED WORK

In this section we provide a short introduction to work in the area of social networking and the technologies that have made it possible.

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, distribute 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 distribute their 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.

Jan Nagy and Peter Pecho [54] has compared two groups of fictive profiles and studied their success in creating new links in social network, also considered tools for protecting sensitive information in social networks. In this paper, testing methodology has used for better protection of sensitive information on social networks and provide the several ways for improve social network security, and established the several precautions as personal precautions (P), technical precautions (T), and user's precautions (U) for security purpose. They conducted a test of social networks users in order to find out their awareness of protecting personal information. At first we proposed personal precautions that require cooperation of user. Then we discuss technical tools and at the end there is a combination of both mentions techniques and administrative and legislative regulation.

Results show that successfulness in creating new contacts is independent on number of current friends. This is proof that they cannot expected users to deal with reputation. Next they compared the differences of creating new contacts with males and with females. The comparison of their results and results of analogical study conducted by Sophos, that tested Facebook users' behavior in Europe.

Pratibha Jagnere et al. [1] has discussed about the possible building malicious applications in social networks and went an application that can launch DDoS attacks using a social network. The main goal of this report is to highlight possible miss-uses of current technologies deployed in social networks. Social networking websites has to provide space on their own servers to application developers to develop their applications so that they can scan them whenever required.

They experimentally evaluate the power of a JPGvirus. Specifically, they explore the effect of placing a malicious Facebook application, which exports view image from shared image server requests to a victim host.

Hongxin Hu et al. [2] OSNs often use user relationship and group membership to distinguish between trusted and untrusted users. For example, in Facebook, users can allow friends, friends of friends (FOF), groups, or public to access their data, depending on their personal authorization and privacy requirements. Users unfortunately have no control over data residing outside their spaces. When a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo, even though the tagged friends may have different privacy concerns about the photo. Stakeholders (tagged friends) don't want to share their information with public. In this paper, they pursue a systematic solution to facilitate collaborative management of shared data in OSNs. They produce a Multiparty Access Control (MPAC) for sharing the data on OSNs can undermine the protection of user data. Their (MPAC) model contains a multiparty policy specification scheme. The use of an MPAC mechanism can greatly enhance the flexibility for regulating data sharing in OSNs.

Ezinwa Okoro et al. [3] 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. [11] 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.

Chalee Vorakulpipat et al. [4] 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.

Balkrushna Potdar et al. [5] that Social networking is used in and outside every organization. There are many social networking whites as sites as facebook, twitter, orkut etc 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.

Prateek Joshi et al. [6] 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.

Jacob W. Keister et al. [7] 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.

Wajeb Gharibi et al. [8] 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.

R. Wallbridge [9] 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.

Abhishek Kumar et al. [10] 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 [12] 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 [13] 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 [14] 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.

Racha Ajami, et al. [16] have surveyed that everyone are focusing on protecting user's information but they have failed to cover other important issues. For example, Users 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, which flip in achieving acceptable levels of security for the social network providers and users.

Waad Assaad, Jorge Marx Gómez [17] 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.

Amre Shakimov et al. [18] 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.

Wenbo et al. [19] have used foursquare as an example to introduction location cheating attack, which easily pass the current location verification mechanism. Authors have also crawl the foursquare website. After analysing 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.

Julien Freudiger 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.

Wei Wei et al. [21] 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. [22] 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, and 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.

Our propose research mechanism depends upon MPAC policy evolution process on depicted in figure 1.

In figure 1. MPAC evaluated in step by step flow chart. Initially an access request goes to under policy evaluation, which is done under four controllers.

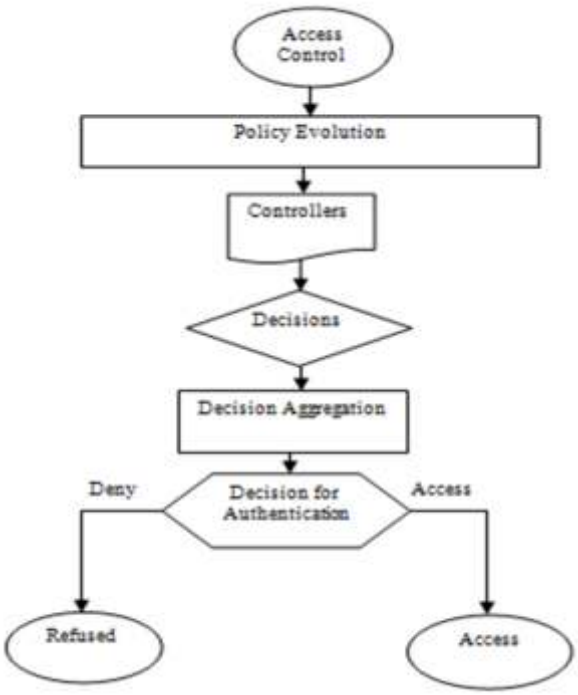


Fig -1: MPAC Policy Evolution Process [2]

It has four controllers they provide their own privacy policies in the form of decision either permit or deny in step-1 process. After giving decisions by individual controllers, they are aggregated and make final decision by using decision voting schemes in step-2 process. The final decision making decides whether the access request is allowed or refused.

3. ALGORITHM FOR SECURE MULTICAST NETWORK:

This algorithm is proposed for providing the privacy on multicast network. In our research work, proposed algorithm provides significant privacy with the design of effective GUI.

This GUI is more users friendly, simple and easily understandable.

Input: Data (d)
Group (g)

Output: Secure data on groups (s)

STEP 1: Data d[0], Group g, Str3, Str4, Con

STEP 2: Initialize Data d with blank space

STEP 3: Initialize Group g with Data d

STEP 4: Set Str3 = d + privacy

STEP 5: Set Str4 = [SQL query Group by Other Person]

STEP 6: Create Connection with database Con + Str4.

STEP 7: Pass the Query Con + Str3

STEP 8: Execute query of step 6

STEP 9: Now fetch value from exe (step 8)

STEP 10: End

4. PROCESS DISTRIBUTION:

As a user distributes their data on a group and multiple users are added in that group, every member of that group are able to share of user's data.

As we know that at the data uploading time on facebook, we use the privacy and provide the permission that whose friend may be view our data or not.

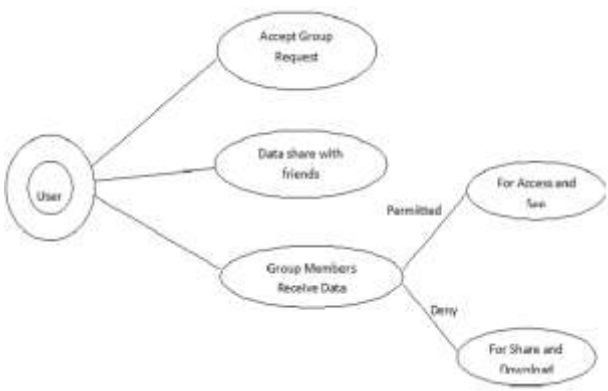


Fig -2: Multicast Grouping Model

We can use the MPAC model (a technique) to put the privacy within the group and can design an

algorithm in the group privacy concern so that, according to figure 2. the users from the joined group only can use and see the data. Joined person can't distribute the group's data outside the group.

So, we want that group members only see the data but not able to access.

5. SYSTEM MODEL FOR SECURE MULTICAST NETWORK

This is the complete system architecture for securing the multicast networks of our whole research work.

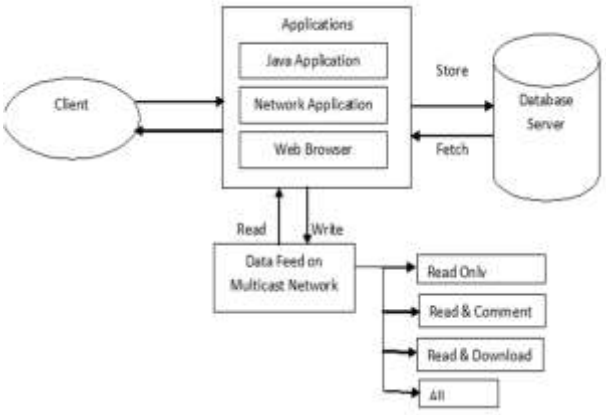


Fig -3: System Model

Client: A client is a person who uses a computer or network service. A client often has a user account and is identified by a username. Other terms for username include login name. Client is an end user who feed their query on the application.

Application: Application is a platform through which end user works. Application follows the work as Java application, Network application and Web browser.

Java Application: Java Application is object oriented programming language and it is a high level language.

In this model Java applications converts the queries into Java Virtual Machine (JVM) Language and also provide the interface.

Network Application: Network Application is a program that lets more than one user open the same data file at the same time.

Web Browser: A browser is software that is used to access the internet. A browser lets you visit websites and do activities within them like login, view multimedia, link from one site to another.

Data Feed on Multicast Network: Client feeds the data on multicast network through the application. At the time of data feed user have the many options as read only, read & comment, read & download and public for securing their information among the multicast network.

Database Server: A database server is a computer program that provides database services to other computer like Oracle and MySQL.

In figure 3, we have provided some important privacy options only for group posts. Because posting data with the modification of actual data on groups are becoming the main problem. So, in this work, we have tried to resolve this problem.

6. WORK ON PLATFORM

The proposed work is implemented in JSP [24]. 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 [23] 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 JMeter may be used to test performance both on static and dynamic resources [25].

7. RESULTS

A snapshot of main interface of my friendbook.com website through this we have done our proposed work as shown in figure 4.1. Photos are loaded into the interface and to control the modification, owner of data choose the options those options are provided by us. If owner of data don't want that his friends share

his data. So, owner sets the privacy according to the data. Through this work, any group member wants to do anything with owner's data,

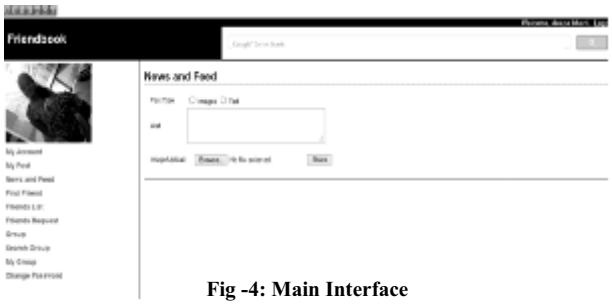


Fig -4: Main Interface

if they would be need the permission of owner. Without owner's permission anybody would not be able to do anything with data.

Privacy options are shown in figure 4.2. These all are that options that are developed by us. Through these options we controlled the sharing and modification with the data on group.

Fig -5: proposed privacy options

Because in facebook we all know that it's have many options through these we our data is secure. But still users want more privacy for data sharing on multicasting networks/groups. Because some person shares data with outside the group and some person do the modification with downloaded data and upload that on other/same group.

So, here users need more privacy because in this situation actual data is not actual. So, that we have developed more these options for multicasting networks.

Fig -6: Post Data

At the data posting time on group we have more options as compare to previous site as facebook.

In this we have create two types of data like image and text as shown in figure 4.3. Choose one data type and then choose privacy option as you want. So, after choose these options we select the data from your computer and then upload. For example: User chooses image type data and privacy is read only. So, in this condition our data is secure. Because nobody is able to share, download, comment and any type of modification with data, actual information will be distributed with our friends/group members. Nobody would be able to harm of owner's data.

Fig -7: Read Only

If anybody wants to download, view, save and comment so, they will be failed as shown in figure 4.4 because in this user have blocked right click event.

If we choose this option for data, group members only permitted for getting the information from that data but not permitted to do any updating with the data.

Fig -8: Read & Comment

If user choose another option as read and comment and then upload the data on any group as shown in figure 4.5. So, it means that user permit only for read and comment to his group members/friends but not for download. Because through this user shares information through the data and get the views of friends regarding that data.

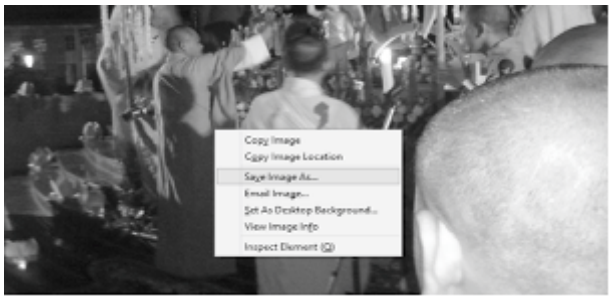


Fig -9: Read & Download

Fig 4.6 If user wants that his friends should have be his uploaded information. So, he selects the read and download as shown in figure 4.6, everybody would be able to download that information and distribute again with others.

Fig -10: All/Public
(Group members have authorization to do anything with data)

Users give the permission to do anything with their data to group members as shown in figure 4.7. In every condition, group members would be need the permission of owner of data to do anything.

So, we have analyzed that after these options our data will be properly secure on social networking sites/facebook.

In this we have add that if anybody download the data on groups/owner's profile. So, owner will get the detail of that downloader person. Through this we would have the detailed of every downloader.

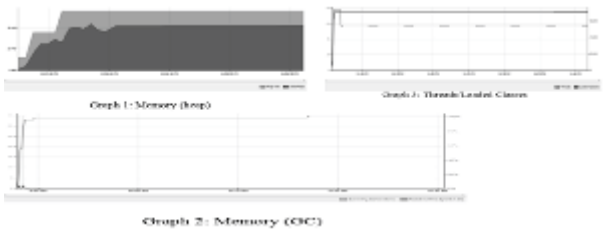
Fig -11: Search Engine

Every social networking sites has their own search engine. There sites search only beyond their space not outside. So, in this we have add a globally search engine as shown in fig 11.

Now we don't need to go another page. It works like google and also give the result like that.

8. RESULTS ANALYSIS

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



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 70 megabytes. Of that about 55 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.

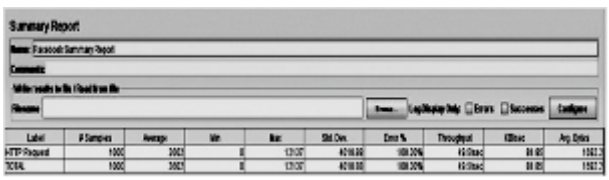
The graph 3, shows the count of active threads in the JVM.

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.

1. COMPARISON BETWEEN FACEBOOK AND SSNETWORK (PROPOSED WORK)

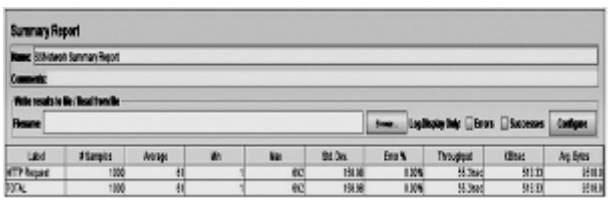
In this we have analyzed the two sites as facebook and proposed work. Through this analysis we can measure the difference facebook and ssnetwork (proposed work).

Table -1: Facebook Summary Report



In the facebook summary report we have taken 1000 samples (threads) to test the facebook. This table showing 3602 average load classes at 1000 samples and in this standard deviation is 4018.88, throughput is 49.5 per second. And working time is 81.85 KB per second.

Table -2: SS Network Summary Report (Proposed Work)



In the ssnetwork summary report we have taken same sample like facebook as 1000 samples (threads) to test the ssnetwork. This table 61 average load classes at 1000 samples and in this standard deviation is 158.98, throughput is 55.2 per second. And working time is 513.33 KB per second and average bytes are 9518.0.

We have proposed our work on JSP with MYSQL database and facebook is in PHP with MYSQL. JSP is more secure than PHP because JSP is much more powerful, since it has access to all the Java libraries. PHP only has access to PHP libraries. Through this testing we can analyze that our proposed work is better than facebook because standard deviation of proposed work is less according to facebook.

9. CONCLUSION AND FUTURE WORK

We have discussed a solution for collaborative management of distributed data in OSNs. We have proposed a multicast model for distributing the data. In which users share their data on group for multiple users. Our experiment will proved low users awareness securing user's data, and group members will not permitted for share and download the data, they are only permitted for view and accessing. In this we have provided a search engine that searches globally and it searches just like as Google. For user we have provided a secure environment. Now users will not afraid of setting up their personal information such as address and other personal information on groups, because now users have the ability to control the sharing and modification over the data. In this dissertation we have tried to resolve modification problem with data on groups by giving the some privacy options.

In the future work, we can design a mechanism for multicasting because it is becoming a dangerous problem for everyone. Through this our friends can harm us and everybody can play with our data. On the social media, users upload objectionable data on multicast network, and data may be anything it may be related to anybody politicians, celebrities and normal person. Some users upload data on social media

for information on group but any group member download that data and after modification again upload on social media. So, through this our culture harms.

REFERENCES

[1] Pratibha Jagnere, Amarnath and Shashi Khosla, "Vulerabilities in Social Networking Sites", 2nd International Conference in 2012.

[2] Hongxin Hu, Gail-Joon Ahn, Jan Jorgensen, "Multiparty Access Control for Online Social Networks: Model and Mechanisms," IEEE Transaction on Knowledge and Data Engineering, July 2013.

[3] Ezinwa Okoro, Stelios Sotiriadis, Nik Bessis, Richard Hill, "Customized Profile Accessibility and Privacy for Users of Social Networks," Third International Conference on Emerging Intelligent Data and Web Technologies, 2012.

[4] Chalee Vorakulpipat, Adam Marks, Yacine Rezgui, Siwaruk Siwamogsatham, "Security and Privacy Issues in Social Networking Sites from User's Viewpoint", IEEE Conference in 2011.

[5] Balkrushna Potdar 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.

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

[7] 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.

[8] Wajeb Gharibi and Maha Shaabi, "Cyber Threats In Social Networking Websites", International Journal of Distributed and Parallel Systems in 2012.

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

[10] Abhishek Kumar, Subham Kumar Gupta, Animesh Kumar Rai, Sapna Sinha, "Social Networking Sites and Their Security Issues", International Journal of Scientific and Research Publications in 2013.

[11] Ping Zhang, Arjan Durresi, Yefeng Ruan, Mimoza Durresi, "Trust based Mechanisms for Social Networks," Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, 2012.

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

[13] Justin Becker and Hao Chen, "Measuring Privacy Risk in Online Social Networks", W2SP in 2009.

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

[15] Jan Nagy, Peter Pecho, "Social Networks Security," Third International Conference on Emerging Security Information, Systems and Technologies, 2009.

[16] Racha Ajami, 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.

[17] Waad Assaad, 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.

[18] Amre Shakimov, Harold Lim, Ram´on C´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.

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

[20] Julien Freudiger, Raoul Neu , Jean-pierre Hubaux, "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] Wei Wei, Fengyuan Xu, Qun Li, "MobiShare: Flexible Privacy-Preserving Location Sharing in Mobile Online Social Networks" INFOCOM, page 2616-2620. IEEE, (2012).

[22] Wei Dong, Vacha Dave, Lili Qiu Yin Zhang, "Secure Friend Discovery in Mobile Social Networks" INFOCOM, IEEE, 2011. "History of MySQL"

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

[24] 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.

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

Jmeter.apache.org. Retrieved 2013-09-20.