International Research Journal of Computer Science (IRJCS)
Issue 06, Volume 6 (June 2019)
SPECIAL ISSUE - 5th International Conference - "ACCE – 2019"
ISSN: 2393-9842
www.irjcs.com

RESTRICTING THE OWNER IN SHARING THE CO-OWNED DATA OF STAKEHOLDERS

Srikantaiah K C, Pooja Kumari, Monisha P, Usha A
Department of Computer Science and Engineering,
SJB Institute of Technology, Bengaluru, Karnataka, India
srikantaiahkc@gmail.com,, pthakur5588@gmail.com, monishaismoni@gmail.com; ushasheki1998@gmail.com

Manuscript History
Number: **IRJCS/RS/Vol.06/Issue06/JNCS10084**
Received: 29, May 2019
Final Correction: 30, May 2019
Final Accepted: 02, June 2019
Published: June 2019
doi://10.26562/IRJCS.2019.JNCS10084
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract—Online Social Network is the network of people connected with the help of internet in the form of cluster of people. In this people are basically related to each other with some relationship types such as Family or Friends or with people to permuting of products. Owners are the one who is having co-owned and stakeholders are the data are being shared. To solve his/her purpose the owner will misuse the data of Stakeholder's by posting it some sites where the stakeholder's account will not be there for these situation privacy policy should be there to restrict the owner in that situation privacy may be compromised since the document can be approached by different users in network. OSN helps users to give the authorized access for the data Sharing. When users decide to post a data, it will be based on the combined opinion of all involved users. Floyd Shortest path algorithm is used to calculate the distance between the users's which further helps in calculating the trust values of each node. We proposed an algorithm called security of trust which helps the stakeholders for misusing of the co-owned data. The trust values between owner's and stakeholders are used to opinions, and accordingly the trust values are updated according to users' privacy loss and it also provide additional for the security of Online Social Network to reduce the leakage of information to the other security trade of between data Sharing.
Keywords- Privacy; Online Social Network; Trust; Data Sharing; Floyd Shortest Path;

I. INTRODUCTION

The popular Online Social Network services such as Facebook, LinkedIn, Twitter, basically these all are the social network providers who allow the users to share the data to the stakeholder's and the opinion of the users to the post the data with the aggregated opinion of the stakeholders. Various OSN applications are developed to satisfy the different peoples opinion based on privacy. Everyday billions of OSN users post data about their daily lives or for the advertisement purpose in terms of text messages, photos, or videos. Those data often include sensitive information of individuals. If the information can be accessed by unauthorized user's, stakeholder's secrecy will be compromised. The privacy issue has always been a major problem in Online Social Network. The privacy control mechanism only imposes the restriction of who can view the data, but they can't impose the rigid regulation on who can post the data. A consequence of this one-side regulation is that the user who posts data may accidentally discard privacy. Strong traids or strong connection are the one who is having more number of friends in the network and on the other hand weak connection are the one who is having the single connection in the network as shown in the Figure1 we can conclude from the them is that if the B's information is leaked from the group to group A then only one of the friends is misusing the data because only one friends are connected to them with weak traids. If that one friend is the owner of co-owned data and he can easily misuse the data. Suppose that a user A's friends wants to sell some of his product and A's will post some advertisement about the product and without asking his/her friends if B wants to buy the product then B cannot communicate directly to that person A act as the broker in that scenario stakeholders privacy will be compromised.

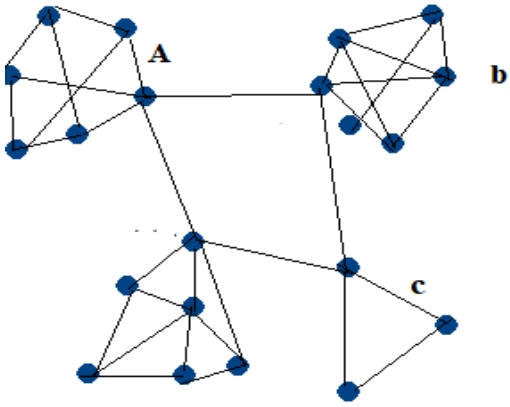

Figure 1: A Social Network

Data which are co-owned by multiple people are very common in OSNs. The user who posts the data will tag all the other attached users. The tagged people can be identified via some techniques (e.g. face reorganization or two step verification). In such case, the intermediary people are able notify about connected users about the posting of the data. However, in Now a day, it is likely that the user posts the data without tagging other users and the involved users are difficult to be identified automatically. Considering this, we have given a mechanism which requires the user to take other's opinion also if the data is co-owned by the users. In this case we will be setting the threshold value if the data is sensitive or insensitive by this method stakeholder's privacy will not be violated. Given the information a user wants to post, and the restriction policy prescribed by the user, every attached user should "vote" to state whether he/she approves of the restriction policy. The vote depends on the trust value between the two users' only when the vote certifies the condition in the OSN then only data can be posted by the owner. If owner tries to violate the policy the trust will decrease. The trust value is mutable parameter it will vary if the trust between users will change. It specifies two mechanisms if the data, they are having is family members data or friend's data. And trust value which we model this problem as threshold selecting problem as the decision-making problem. Online social networks are a platform where large number of users interacts with each other. That is, they can chat, share photos either to an individual or in a group and even post photos online which everyone can see. In simple its nothing but it comprises of large number of people or organizations who communicate that is interact with each other. Nowadays online social networks are very much useful as it allows users that are friends to stay in touch with each other. As they can stay in touch through these networks by texting each other video calling etc. But also, they are problems related to these networks such as privacy loss can occur to the user. This problem mainly arises when it's a co-owned photo or the data. Co-owned in the sense when the data involves many users in the network. To overcome this problem, we use many techniques for the data sharing and simulation.

- Improve and extend the Floyd Shortest path algorithm to find out the shortest path between the nodes and generating the weight adjacency matrix to updating the value.
- A trust-based policy is used to maintain privacy in online social network. The trust value between the user's privacy loss.
- Data sharing and simulation is done to clean the dataset and get useful information from the nodes like how many nodes and datasets are there between the nodes.

The rest of the paper is organized as the follows section II gives the related work. Section III gives the System Architecture .We introduce the knowledge about the creation of Online Social Network and related concept used in developing the model and our approach in Section IV. Section V describes the experimental results. Conclusion is done for the paper in Section VI.

II. RELATED WORK

Trust-based Collaborative Privacy Management in Online Social Networks [1] in this mechanism, threshold is been introduced on which the stakeholder's makes the final decision on data posting by the voting scheme. Basically, this problem was first investigated by using game theory. After that users are willing to negotiate and make agreement to achieve the restricting policy is reproduce and it should definitely satisfy certain condition. The concessions that users may be willing to make in different situations are modeled as a set of concession rules, and a computational policy is to solve the privacy conflicts. Basically, *in different privacy method hence it will change with* time. trust plays a crucial rule in network application.such peer to peer network(P2P network.Trust based access control utilizes the trust value to point out how much impact a user opinion to be there on aggregated decision making while in different restriction method Trust values in the user's secrecy loss, hence they can change over time. In Information Dissemination,[12] models the speed and scale of information dissemination they have neglect the reciprocal propagation between communication between the candidate.

Further implement analytical models based on discrete processes. These models still cannot be applied for the use of real cases since many influential factors have not involved in the cases. A robust, large-scale algorithm to de-anonymize[4] online social network data. Their approach is based purely on the network topology, and works in a self-reinforcing, feedback-based manner.

III. SYSTEM MODEL

A. Problem Defination:

The basic problem in Online Social Network is to provide the Security to the sensitive data item posted by the OSN user's in the day to day life.If the data is misused by the owner then it is privacy loss for stakeholders for that we have proposed the Security of trust algorithm to restrict the owner in sharing the co-owned data by the owner because he can probably misuse the data item in some other websites.

B. Creation Of Online Social Network

An Online Social Network can be represented as G=(V,E), Where V is the set of user and E is the set of the edges and RT is the set of relationships between the two users. When we replace the directed edges with the undirected edges then the distance is calculated between the two users. After creating the graph with the networkX Package. Floyd-shortest path function was built in function was provided in the python to calculate the distance between the two nodes. When there is no path between two vertices v_i, v_j and the distance between them $D_{ij=\infty}$. Where D is the distance between the two owner and stakeholders. This helps calculating the trust between the owner and stakeholders. When the network is created, we can assign the threshold to each relationship and it is tunable parameter *i.e* it can be changed according to trust value between owner and stakeholders.

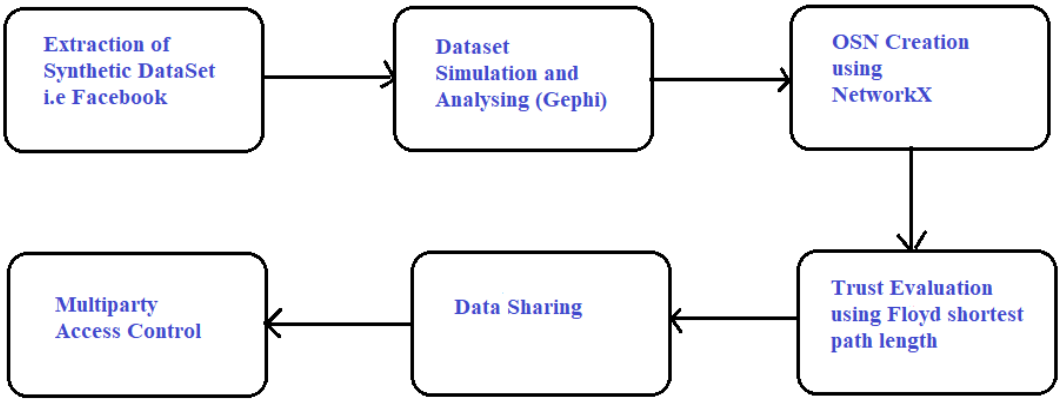

Figure 2: System Architecture for restricting the Owner

C. Data Sharing

Data sharing is nothing but the act of sharing information with two users or multiple users through an online social network. And this data shared should be encrypted. And only the intended user is supposed to get that data. There should not be any privacy loss to the owner who is sending the data.so the data should be secured and encrypted before sending it to the user such that there should not be any privacy loss. Data can be encrypted using the various encryption algorithms. Data sharing can involve either the sharing of photos, videos or sensitive information in the form of messages etc. And data sharing can be done with two or more users in the online social networks. And the data can be shared individually or in a group.

ALGORITHM 1: Simulation Algorithm

Purpose: To find out the owners and the stakeholders in the network.
Input: created network.
Output: obtained the owners and the stakeholders.

Step 1: To find the owners in the network by setting a $prob_i$ value
$Prob_i$ < threshold value
Then user acts as the owner otherwise user does not act as the owner
Step 2: To find the stakeholders
Randomly select stakeholders to the owners
Setting Average node degree=8
Result: Then every owner has 8 stakeholders. Distance between the nodes should not be greater than the threshold distance then user can access the data posted by the owner Otherwise cannot access the data.
Step 3: End

The advantage of data sharing algorithm is that we can find out the total number of owners and the stakeholders in the network and the disadvantage is that We cannot select the desired stakeholders. As the stakeholders will get generated randomly. Either a message, audio, video or a photo. So, for this we first found out the total number of owners in the network. And the number of people who are directly connected to the owners that is the stakeholders. And we have set the average node degree to be 8. So that means every owner has eight stakeholders with whom he or she can share the data. We found out the owners by setting a $prob_i$ value that nothing, but users will be generated randomly and uniformly in the range 0-1. And we set a threshold value. And when the $prob_i$ value is smaller than the threshold value those users are selected as the owners from the network which we created. And when the distance between the nodes in the network is not greater than the threshold distance then those users are considered to be the stakeholders. Threshold distance is nothing, but the distance set randomly. So, this way we have found out the owners and the stakeholders in the given network. And when the owner is not willing to share the photo with all the stakeholders, he can restrict the access with only few stakeholders by using the multiparty access control. Where a threshold value is set and only the users who satisfy that threshold value can view and access the data. That is the authorization permission is given to them. Only the users who satisfy the threshold value will be authorized to view any kind of data posted by the owners. All the unauthorized users will get restricted to access the data posted by the owner and cannot view them. We are simulating the data in the network to find out the total number of the owners and the stakeholders in it. And we display the names of the owners with the corresponding stakeholders. And the showing the data sharing behaviors between them that is how the data will get restricted. When the users who doesn't satisfy the threshold set by the owners those users do not have the authority to view the data posted by the owner. And get restricted from viewing it. Only the users with the access threshold value say 0.8 is there only those users can view the data posted by the owner that is they are authorized to view the data posted by the owner.

D. Finding the owners and the stakeholders

Here we are simulating the data in the network which was created to find out the total number of users in the network and which user is acting as the owner and who is acting as the stakeholders. So firstly, for finding the owners the owners will get generated randomly from the values 0 to 1. And a $prob_i$ value is set. And when the $prob_i$ value is lesser than the threshold value then those users' acts as the owners. The threshold value is set randomly. By this way the owners are obtained from the network. And after the owners are obtained, we need to find out the stakeholders for that owner. The stakeholders are found by the random generation and we have set the average node degree to be 8 so that every owner has 8 stakeholders.

E. Trust Evaluation

Trust plays a very important role in Online Social Network (OSN). Users in the network are connected to each other directly or indirectly. A user which is connected directly is said to be closely related to each other and the distance between the users is less. The distance between the users connected either directly or indirectly is calculated by using Floyd Warshall algorithm, which gives all pair shortest path between every user in the network. The distance calculated between users helps in further calculation of trust values in the network. If the owner considers the stakeholder's opinion before posting the data. In such scenario whether stakeholders suffer privacy loss depends on the final decision taken by the owner. For this situation we train the model in such a way that it adopts voting scheme to aggregate the stakeholder's opinion. Then the trust values(T_{ij})between two users V_i and V_j is calculated. In eqation *i* we have used binary value to that weather he/she approves the owner privacy policy 0 means disapproval and 1 means approval of the post as shown in the equation 1.

$$T_{ij} = \begin{cases} 1 & Owner\ accepts\ the\ post \\ 0, & otherwise. \end{cases} \text{----------(i)}$$

If two users are directly connected to each other the trust is set to a positive constant say 0.8, which is the trust value being set between the users. If the users are not directly connected, then the trust value is evaluated using 0.8^d where d is the shortest path length been calculated using Floyd_warshall algorithm. The initial value of trust is calculated using this method. For further calculated of trust the value need to be updated.

F. Multiparty Access Control

The Online Social networks, such as social media like, Twitter, WhatsApp, Facebook, and People will share the data or information with friends, family members, co-workers, So safeguard shared data in OSNs defining a Multiparty Access Control And The OSNs the Multiparty Access Control is a process of protecting the shared data in the network. In this access control method will allow the users to access the information in their own space, But the outside of their space in the network there is no control over an access for a data. And she/he cannot specify which user can see or view the data that shared in OSN. And also, whenever a user uploads any image in an OSN and also, she/he can tags to his friends who are become visible in the image so the connected friends can't set any limit for the access for the data, who can see this image and who cannot. Despite the fact that connected friends may own different privacy method about the data or an image so defining a multiparty Access Control for the shared data.

The users or the people in the OSNs will allow to limit the access to a data that is shared in OSNs, in order to protect the their privacy in the OSN, But they do not provide any technique or any method to apply privacy over a data linked with a multiple users so here prefer an method to enable the safeguard of a shared data and prevent the loss of privacy. The Multi Party Access control in Network is providing an access control policy scheme for the data, that is shared in an OSNs, means define a policy like access control to prevent the loss of privacy for the stakeholder and the owner. The owner is, one who share the data in network, so he/she will be owner of the data, and the user is nothing but one who try to view the data, which is originally posted by others. The stakeholder will be selected, based on the trust value from the owner to user if the trust value is high the user will be defined as stake holder, if not the user is not the stake holder for the owner. After the stake holders are selected the authorization will be defined for the stakeholder, means who can view the data and who cannot view the data which is shared in the network. So by defining the authorization for the stakeholder the owner privacy will be secured, and preventing the privacy loss to the owner by defining authorization for the stakeholder, the data can only accessed by the authorized stakeholder, unauthorized stakeholder will not see the data or they can't view the data which is shared in the network by the owner.

ALGORITHM 2: Access control policy for data

1. Purpose: Defining access control policy for the shared data
2. Input: Synthetic Facebook dataset
3. Output: Access control for shared data

Step1: Finding owner and stakeholder in simulation Algorithm
Step2: Owner will share the data in OSNs
Step3: Define access control policy for the shared data
Step4: Stakeholder try to access the data
Step5: Access permission for stakeholder
Step6: If stakeholder trust value is equal to owner trust value the access permission will be given
Step7: If the stakeholder trust value is less the access permission will be denied

The Advantage is securing the privacy of the user in OSNs that is by defining privacy policy and setting access control policy for shared data. The Disadvantage is user cannot define access control policy for the data that is already being shared by linked user in OSNs because every user has their own privacy policy. For the owner after the stakeholders are selected the authorization will be defined for the stakeholder, means who can view the data and who cannot view the data which is shared in the network. So by defining the authorization for the stakeholder the owner privacy will be secured, and preventing the privacy loss to the owner by defining authorization for the stakeholder, the data can only accessed by the authorized stakeholder, unauthorized stakeholder will not see the data or they can't view the data which is shared in the network by the owner.

ALGORITHM 3: Security of Trust (SOT) algorithm for the stakeholder's privacy loss.

Input: Fetch the Owner dataset to model and create the weighted graph from the dataset where $O_{i=1,2,to\ N}$ is the owner selecting one owner and S_i is the stakeholder's
Output: The stakeholder's privacy security will come in the form of 1.
Purpose: It will solve the stakeholder's privacy if the owner wants to misuse the data.
Step1: Calculate the shortest distance from the dijkstra's_path_length function and update the value to dist_value. Otherwise update dist_value=999;
Step2: Setting the threshold values for the owner threshold=0.8 opinion threshold=0.5, dist_threshold=0.32, access
Step3: Then call the Data sharing algorithm 1 to check whether it is authorized or unauthorized users.
Step 4: For checking the stakeholder's privacy loss trust values should be between 0 and 1.

```
if stakeholder== 0:
        g_of_ls=1;
    else:
g_of_ls=(2*(e**stakeholders_loss)1+(e**stakeholder_loss))
if g_of_ls=0:
```

Step5: new trust values will be updated and if it is new trust values should be greater than 1 the it will be updated with 1.0.and call the access control algorithm

```
 if aggregated_opinion>opinion_threshold:
  Print stakeholder's soliciatated your post
 else:
```


Print stakeholders rejected your post
Step 6.Return the opinion to the owner.
END

The privacy secure for the stakeholder in online social network, for that there is a voting technique in network, while the owner posting the data like an image, video in that data, it contains stakeholders data also means in an image the stakeholders image will be there, while the owner posting the data he/she has to ask stakeholder permission for that there is voting technique is there while the owner is posting the data the stake holder will vote for the data means the data can be posted or not based on the voting technique the data posting the network will be decided, if the stakeholder vote is positive means the owner can post the data ,if the stake holder vote is negative means the data cannot be shared in the network. So the owner as to ask for the permission, but also sometime the owner will post the data item in the network without asking the permission from stakeholder, so the owner does not care about the stakeholder privacy in the network, so the stakeholder will suffer the privacy loss in the network.

IV. EXPERIMENTAL RESULTS

We conducted simulation on the synthetic dataset of Facebook collected from the SNAP repository. The simulation is performed with the help of software Gephi *i.e. supported higher version of JAVA* as shown in the Figure 4.1 .The network is a scale free network contains 4039 nodes and average node degree was 12 as shown in the Figure 4.2 it means that one person in the Facebook have average 12 friends and clustering coefficient is 0.276 as shown in the Figure 4.2 and it also containing 88234 undirected edges. The software which we have used for the development of the Trust Based Model are gephi is an open-source software for visualizing and analyzing the Online Source Network (OSN). Basically, it is used for 3d graph and for analyzing the different properties of the Graph. Pycharm gives us the basically access command line, connect to the database. It is developed by JetBrains.Pgadmin3 to maintain your PostgreSQL database. The hardware requirement for developing the projects are the processor should be P4 and above, the RAM is 1 GB, the graphics above HD 500GB and above. The external device which we are using is Optical Mouse, Standard Keyboard.

Simulation Results are as follows.

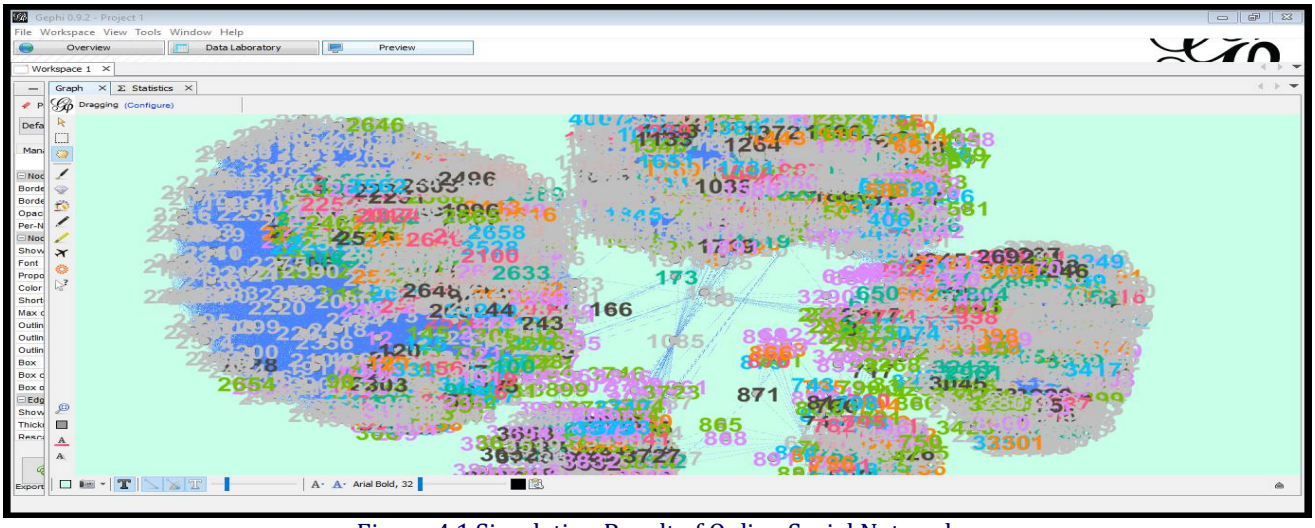

Figure 4.1 Simulation Result of Online Social Network

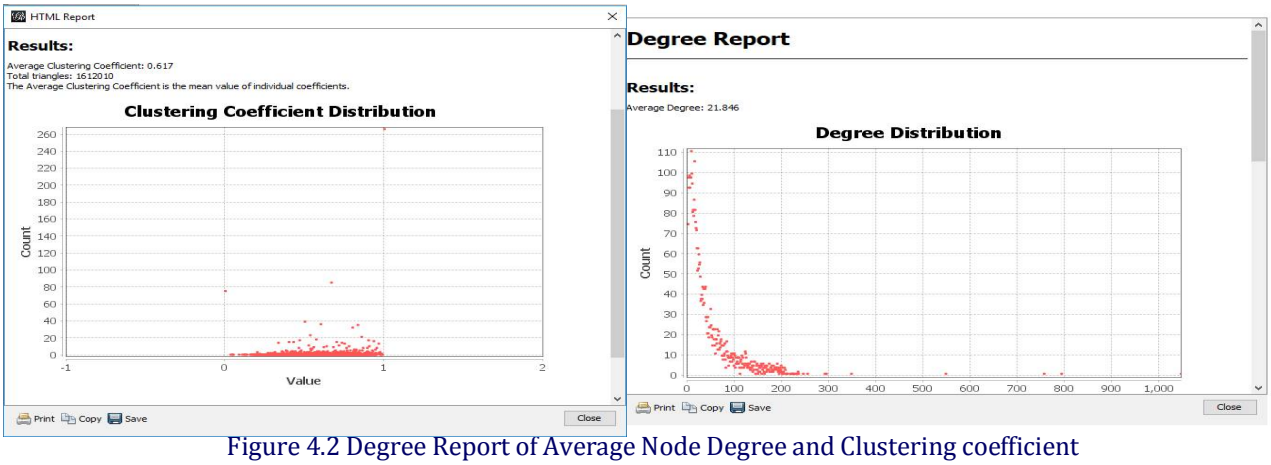

Figure 4.2 Degree Report of Average Node Degree and Clustering coefficient

V. RESULTS

Online Social network service providers give the built in feature for only imposes the restriction of who can view the data, but they can't impose the rigid restriction on who can post the data. A consequence of this one-side restriction is that the user who posts data may unintentionally violate another users' privacy. Consider the example where the photograph contains the picture of three users. Lingo, Parul, Paul if Parul uploads the photo and she has not tagged Lingo, Paul so basically Lingo, Paul privacy is compromised. For this type of privacy loss, we have introduced mechanism to control the privacy and it should be based on the trust value between the users and stakeholder's before posting the co-owned data he has to ask the stakeholders to vote.

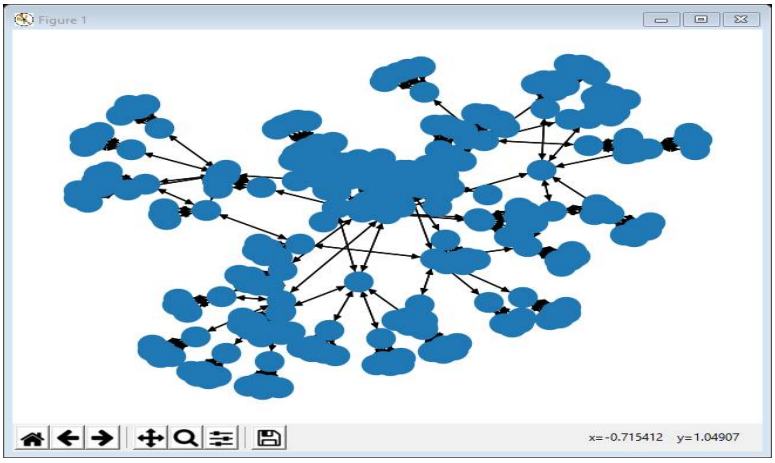

Fig 5.1 : Creation of Online Social Network

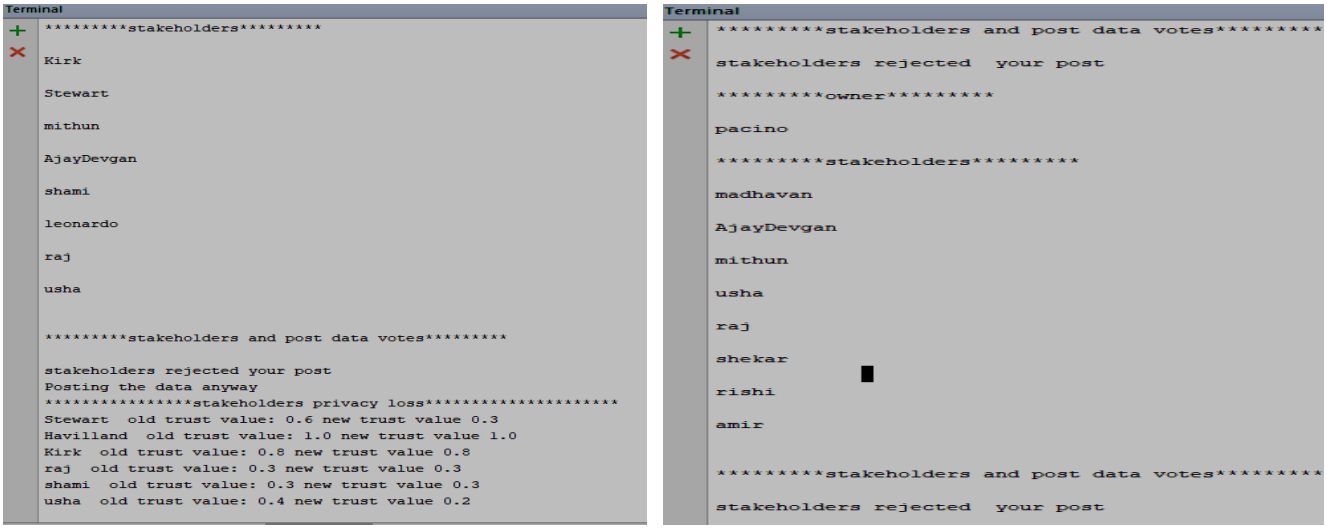

Figure 5.2 output of Trust Based Model for OSN

Owner Oi	Stakeholders Si	old trust	new trust	privacy loss
Usha	marlen james mitchan sami raj usha Mithun	1.0 0.6 0.8 0.3 0.3 0.4 0.4	1.0 0.6 0.8 0.2 0.2 0.2 0.4	0.6
Usha	marlen james mitchan sami raj usha Mithun	0.6 1.0 0.8 0.3 0.4 0.5 0.4	0.3 1.0 0.8 0.2 0.2 0.3 0.4	0.4

Table1. Trust Result

VI. CONCLUSION

Online Social Network is a platform that is made up individuals and organization termed as nodes and between them is the link that uses internet as the connective medium. In this people are related to each other with some relationship between them such as Friends, Family member or to some remote some product.

The end goals for developing our project is to prevent the misusing of the sensitive data which is co-owned by the user's as well as the stakeholders hence the owner can misuse the information of stakeholder's to some site where the stakeholder's account is not there. To solve this purpose the owner has to ask the stakeholders to share the co-owned data. For this reason, we must set the trust value which is based on the distance between the owner and the stakeholder and it will be calculated based on the formula. In such scenario privacy loss for the stakeholders shouldn't be compromised. Future work should seek to provide to include these all work to include the work to OSN social network to the provide security for OSN.

REFERENCES

1. Lei Xu/Chunxiao Jiang,Nengqiang He, Zhu Han/and Abderrahim Benslimane (2008)Trustbased Collaborative Privacy Management in Online Social Networks IEEE on Information Forensics and Security, vo1.18,pp556-6013,Beijing 2018.
2. Sudarshan Kudlur Satyanarayana, Keshav Sood, Yuan Tao and Shui Yu "Security and Privacy in Online Social Networks: A Survey" 09 December 2014 [3] Gulyas G.G.; IMRE (2014):
3. Measuring importance of seeding for structural de-Anonymization attacks in social networks:IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 , pp.610-615, Budapest 2428 March 2014
4. Huber, M.; Mulazzani, M.; Weippl, E.; Ki, G.; GOLUCH, S. Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam: Internet Computing, IEEE, vol.15, no.3, pp.28- 34.
5. DING X.; ZHANG L.; WAN Z; GU. M. (2010) A Brief Survey on De-Anonymization Attacks in Online Social Networks: International Conference on Computational Aspects of Social Networks (CASoN), 2010, pp.611-615, Taiyuan 26-28 Sept. 2010
6. JOHNS, M.; ENGELMANN, B.; POSEGGA, J. XSSDS: Server-Side Detection of Cross-Site Scripting Attacks: Computer Security Applications Conference, 2008. ACSAC 2008. Annual, pp.335-344, Anaheim, CA, 812 Dec. 2008
7. FAGHANI, M.R.; MATRAWY, A.; CHUNG-HORNG LUNG A Study of Trojan Propagation in Online Social Networks: 5th International
8. Conference on New Technologies, Mobility and Security (NTMS), 2012, pp.1-5, Istanbul , 7-10 May 2012
9. TRIFA, Z.; KHEMAKHEM, M..; (2012) Mitigation of Sybil Attacks in Structured P2P Overlay Networks: Eighth International Conference on Semantics, Knowledge and Grids(SKG), 2012, pp.245-248, Beijing, 22-24 Oct. 2012
10. TRIFA, Z.; KHEMAKHEM, M..; (2012) Mitigation of Sybil Attacks in Structured P2P Overlay Networks: Eighth International Conference on Semantics, Knowledge and Grids (SKG), 2012, pp.245-248, Beijing, 22-24 Oct. 2012
11. HAIFENG YU; KAMINSKY, M.; GIBBONS, P.B.; FLAXMAN, A.D. (2008) SybilGuard: Defending Against Sybil Attacks via Social Networks: IEEE/ACM Transactions on Networking, vol.16 (3), pp. 576-589.
12. WEN, S; JIANG J; XIANG X.; YU, S.; ZHOU, W. (2014) Are the popular users always important for information dissemination in online social networks? : Network, IEEE: vol.28 (5): pp.64-67.
13. WEN, S.; HAGHIGHI, M.; CHEN, C.; XIANG, Y.; ZHOU, W.; JIA, W., (2014) Sword with Two Edges: Propagation Studies on Both Positive and Negative Information in Online Social Networks: accepted in IEEE Transactions on Computers.
14. Lei Xu, Chunxiao Jiang, Nengqiang He, ZhuHan, Abderrahim Benslimane. "Trust-basedCollaborative Privacy Management in Online Social Networks", IEEE Transactions on Information Forensics and Security, 2018.
15. Xuan Ding, Lan Zhang, Zhiguo Wan, Ming Gu. "A Brief Survey on De-anonymization Attacks in Online Social Networks",International Conference on Computational Aspects of Social Networks, 2010.
16. Hu, Hongxin, Gail-Joon Ahn, and Jan Jorgensen. "Multiparty Access Control for Online Social Networks: Model and Mechanisms", IEEE Transactions on Knowledge and Data Engineering, 2013.
17. Sonkar, Shailendra Kumar, Vishal Bhatnagar, and Rama Krishna Challa. "An analogy between static and dynamic social network based on critical parameters", International Journal of Social Network Mining, 2013.
18. tel.archives-ouvertes.fr Int ernet Source Sonkar, Shailendra Kumar, Vishal Bhatnagar, and Rama Krishna Challa. "An analogy between static and dynamic social network based on critical parameters", International Journal of Social Network Mining, 2013.
19. Theepigaa, Th., and A. Bhuvaneswari. "Efficient and contorlled sharing of privacy data in social networks", International Conference on Information Communication and Embedded Systems (ICICES2014), 2014.

