AN EFFICIENT FRAMEWORK FOR PROTECTING SENSITIVE DATA IN SOCIAL NETWORKS

Battula Ravindra Chantibabu[1], Prof.S.V.Achutha Rao[2]

[1]Pursuing M.Tech(CSE), [2]HOD, Vikas Group of Institutions, Nunna, Vijayawada. Affiliated to JNTU- Kakinada, A.P, (India)

ABSTRACT

In social networks we can see the protection to the user's data. Now a day social networks become a part of human life to share everything immediately and to get response from others and to know the information about others these all the things, so when we are sharing in anyone of the social networks we cont trust anyone some of the times it may go to miss usage and any one can see our data. To stop that problem in social networks and to maintain in a good manner and other people means who is the out of his selected people can't see his information on the social networks and to make it be user choice we are making all these things are well inform. For this paper we are proposed a label method for the user based on his selection and his performance only others can see his shared data and his information also no other people can see his information. And here to publish the user shared data we are using privacy protection algorithm for the security purpose. This algorithm has used for the losing of small content of information and to protect the large amount of data.

Keywords: Social Network, Label, Data Sharing, Privacy Protection.

I INTRODUCTION

In general human life we can see how social networks are popular and how it works in. due to these reasons we are securing and providing security to the networking data and in main system of the process the use can register and he can get any information from the other share people. In this middle period of reason we can see how many changes are happening and how the data will modify in the transaction. If we consider the social network information as that we know about it it's a combination of many things and sharing of information which was related to the user's personal information and based on their profiles and this information is a sensitive information in social networks that means the users data whatever he want to make and feel as not share others and to hide to the people is as a sensitive data. So to hide this information and protect his data t non visible to others and all the people we have to follow some of the rules that we can see in bellow.

Now days we can more social networks like face book, linked in, save pages, etc. these all are considered to share the user's data and to check the available information on online. So it is very difficult to provide the security to the user data and for that just we are maintaining only one level based information and that data only can visible to everyone on the social networks for that of the reason here we are taken number of levels like some of the labels we are taken and based on that that labels the user can select for that we are maintain like a groups of labels in the user profiles.

Mainly in this paper we are implemented and proposed a way for the user data protection and we are focusing here for the privacy protection are of the user information and for that we are selecting different types of nodes which will carry the information from one location to other and for that we are having different types of labels for each and every node and through this points of nodes we are making that as a directional path and we are getting the graph. Path of all the nodes information and its related information and there are many ways to hide the nodes information and to store the information. The main thing in this is to share the data from one person to others and not only has all the people but there are some restriction for it to stored the information and its related data and to protect the individual data with the privacy and maintain it for other to be visible as a selected people only that is the challenging position in social networks because now social networks are become very speedup compare to the other website. And the same preserved data we have to share the others by the permissions of the user only for this to maintain and to know this we are implementing graphical phenomena to know the each and every transaction of data in the selected field.

At the same time user may have the non sensitive data information so that can be visible to others. So when we are sharing in anyone of the social networks we can't trust anyone some of the times it may go to miss usage and any one can see our data. To stop that problem in social networks and to maintain in a good manner and other people means who is the out of his selected people can't see his information on the social networks and to make it be user choice we are making all these things are well inform. For this paper we are proposed a label method for the user based on his selection and his performance only others can see his shared data and his information also no other people can see his information. And here to publish the user shared data we are using privacy protection algorithm for the security purpose.

In general structure we can see the attacks in social networks and we can make it to pass each and every node from one to other to prevent and to implement that node of transformation we will use the security preserving methods for the protection of user node information.

II. PROPOSED WORK

In this paper we proposed l-diversity like model, it always checks the nodes with l-1 other nodes. In the proposed system we are providing security to the sensitive labels by grouping the friends, here we are grouping the people in to four categories, 1) collogues, 2) family friends, 3) close friends, 4) friends.

With this grouping we will provide security for our sensitive data like posts, images and some personal information, simply the persons to the site will send request to particular his friend, when the second persons accepting to him as a friend by selecting the category from the given category, whatever the operations we are performing we will do using the group, so other group person will not have the permission to view or access particular post. A user while uploading his images or posts will select a group to give permissions to which group persons has to view his data and download its personals, and remaining persons doesn't have permission to access or view the data, means here we are giving permissions particular persons of friends, here we are following the neighbor nodes concept to protect sensitivity of neighbor nodes, here nodes lets we say friends in the social network anybody can upload his personal information to the site and sometimes this information is threat by others in the previous technique, here we don't want share our secretes with others. To implement this we will give permissions to particular persons from friends, while uploading the information we select persons

to whom we are giving the permissions, only those persons only view your information remaining persons will not have the permissions to view or perform any operations on the data.

III ALGORITHM

The main purpose of algorithms that we have proposed is to make proper group of nodes, and suitable modification of labels of neighbor nodes of every group will satisfy the l-sensitive-label-diversity requirement. We want to cluster nodes with similar neighborhood information labels so that we can avoid some noisy nodes as possible. We will do this with Global-similarity-based Indirect Noise Node (GINN), Direct noisy node (DNN) and Indirect noisy node (INN).

3.1 Algorithm GINN

The algorithm worked on group formation for the nodes which not at all gathered. At first the two nodes having the similar labels grouped together. We calculate similarity of neighborhood labels as follows.

$$NLS(v1,v2) = \frac{|LSv1 \cap LSv2|}{|LSv1 \cup LSv2|}$$

Larger values specify larger parallels of two neighborhoods.

The nodes which are having larger similarity with other nodes in the group are gathered as cluster till the group has l nodes with different sensitive labels. This algorithm proceeds to create next group. After group formation if some l-nodes left from the nodes, those nodes will cluster from the existing group.

After complete these groups formation. We ensure that the neighborhood members will indistinguishable their neighborhood information. Like neighborhood labels modified after group formation operation, so the labels of nodes will updated for next group operation. This modification process is specifying that all the nodes in the group having similar neighborhood information. This will achieved by several modification operations. To do modify graph with as low loss information as possible. We develop three modification operations: label union, node addition and edge insertion.

The Edge insertion is most complement for both insufficient and missing labels degree value. A node will liked other nearby node with labels. The label union adds value of missing label by creating super values, and those shared among the labels of the nodes.

Algorithm 1: GINN

Input: graph G (V, E, L, L^2), parameter l;
Result: Modified graph G'

```
1 While V left > 0 do
2     if | V left | ≥ l then
3       Compute pairwise node similarities;
4       group g← v1, v2 with Max similarity;
5       modify neighbors of the g;
6       while |g| < l do
7           dissimilarity (Vleft, g);
8           group g← v with Max similarity;
9           modify neighbors of g without actually adding
                noisy nodes;
```

10 else if $|V_{left}| < l$ then
11 for each $v \epsilon V_{left}$ do
12 similarity (v, gs)
13 $g_{Max\text{-}similarity} \leftarrow v$;
14 modify neighbors of $g_{Max\text{-}similarity}$ without actually adding noisy nodes;
15 Add expected noisy nodes;
16 Return G′ (V′, E′, L′)

In the above algorithm noisy node adding operation that is trying to expect to make the nodes inside the every group will satisfy the l-sensitive-label-diversity is recorded, but not performed completely. Only after completing basic grouping operations, this algorithm proceeded to perform the expected node addition operation in the final step. That is if nodes have the same labels from those only one will added, means we are avoiding noisy nodes.

IV RESULTS

Here in this application we did an online social network website and we are collected all the information about the user who ever registered in this website and after that in this we are provided some of the labels to the user after he login his profile information he can upload all his details in step by step of the levels and its based information in that we are providing the labels information to the users he can select and add some of the labels to his files and based on that label his profile will be set after that he can search the people and he can check the users profile also and he can accept the friend request from any person when he accept the friend request that time he has to assign the people based on their relationship. In general we have public, private options but here user can add some of more to whom his data can be visible who can access his data based on that when the user given permission to his friends, who ever in his friends list people can only see the data the remaining people can't see his information and as well as they can't share the user information also and like that of user personal information whatever he felt like its sensitive data that data also all people can't see but whomever he select they only can view the data like this we are provided security to the user data and exactly we got the output.

V CONCLUSION

Finally in this paper we are proposed a way protection to the users data and his related sensitive information based on the labels information and the category which was selected by the user when he was registered in the social network and the sensitive information of the user will be visible to the his selected people only not to all the people like of that this application was madden. Here in all the times the sharing of the data has been passed by the nodes and it has taken in to a way of the representation and the concept of overlapping has been involved in this application that all will protect the user information.

REFERENCES

[1] X. Gao, M. P. Singh, and P. Mehra, "Mining business contracts fothe r service exceptions," IEEE Transactions on Services Computing, vol. 5, no. 3, pp. 333–344, Jul. 2012.

[2] H. Tanev, J. Piskorski, and M. Atkinson, "Real-time news event extraction for global crisis monitoring," in Proceedings of the 13th International Conference on Natural Language and Information

Systems: Applications of Natural Language to Information Systems, ser. NLDB. London: Springer-Verlag, 2008, pp. 207– 218.

[3] M. P. Singh, "Norms as a basis for governing socio technical systems," ACM Transactions on Intelligent Systems and Technology (TIST), pp. 1–21, 2013, to appear; available at http: //www.csc.ncsu.edu/faculty/mpsingh/papers.

[4] M. Pasca, "Answering definition questions via temporallyanchored text snippets," in Proceedings of the 3rd International Joint Conference on Natural Language Processing, Hyderabad, January 2008, pp. 411–417.

[5] M. De Marneffe, B. MacCartney, and C. Manning, "Generating typed dependency parses from phrase structure parses," in Proceedings of the 5th International Conference on Language Resources and Evaluation. Genoa: European Language Resources Association (ELRA), 2006, pp. 449–454.

[6] M. Marcus, M. Marcinkiewicz, and B. Santorini, "Building a large annotated corpus of English: The Penn Treebank," Computational Linguistics, vol. 19, no. 2, pp. 313–330, 1993.14

[7] J. Finkel, T. Grenager, and C. Manning, "Incorporating nonlocal information into information extraction systems by Gibbs sampling," in Proceedings of the 43rd Annual Meeting on Association for Computational Linguistics. Ann Arbor, Michigan: ssAssociation for Computational Linguistics, 2005, pp. 363–370.

AUTHORS PROFILE

Battula Ravindra Chantibabu, pursuing M.Tech(CSE) from Vikas College of Engineering and Technology, Nunna, Vijayawada. Affiliated to JNTU-Kakinada, A.P., India

Prof. S.V.Achutha Rao, is working as an HOD, Department of Computer science Engineering at Vikas College of Engineering and Technology, Nunna, Vijayawada, Affiliated to JNTU-Kakinada, A.P., India