An Efficient Identification Security Control Model for Online Social Network by Controlling User to User Relationship

Sujita Ramanujam[1], Iswarya[2] ,Rupa Kesavan[3] and R.K.Kapilavani[4]

[1]*B.E, Department of Computer Science and Engineering ,Prince Shri Venkateshwara Padmavathy Engineering Collage ,Chennai, India*
[2]*B.E, Department of Computer Science and Engineering ,Prince Shri Venkateshwara Padmavathy Engineering Collage ,Chennai, India*
[3]*M.E,.MBA, Assistant Professor, Department of Computer Science and Engineering ,Prince Shri Venkateshwara Padmavathy Engineering Collage, Chennai, India*
[4]*M.E., , Assistant Professor ,Department of Computer Science and Engineering ,Prince Dr.K. Vasudevan Collage of Engineering and Technology, Chennai, India*

Abstract—Now-a-days relationship between User and Resources has been given in the form of user to user relationship in Online Social Network(OSNs). This may play a major role in enforcing and specifying the access control by which the privacy between a user to user relationship has been maintained where there are some polices which are given to the User and Resources in OSNs are in terms of multiple relationship types and requested actions etc.,.In this paper we present a new Identification Access Model which will be controlling user to user relationship. This can be achieved by the use of path checking algorithm, that will determine whether the required relationship between the users exist or not. And if the relationship is not found the that user may control the access of one friend with another one. Additionally we can also perform an option for hiding the profile picture in a particular site for some group of people around the friends circle. This is performed using privacy preserving algorithm.

Keywords—*Social Network, identification access model ,user to user relationship.*

I. INTORDUCTION:

THIS document tells us about the use of Online Social Network that is used by large number of people all over the world and the security that is provided by the OSNs. Some network are used to share only videos. But in some Online Social Networks like "Facebook" not only videos but also all type of information are shared in that network. Many users are joining the OSNs are generally they are connected to each other and share a large amount of information which may be private or public. These information sharing are kept secured since there are more options are available in each OSNs where they provide security and that gives user a privacy for sharing any form of information. The Security and privacy in OSNs are maintained well in both media and research community [1], [10]. These views indicates that there is a need for access control for any unauthorized access over the OSNs. An Access Control in every network there are more unique characteristic that provides more security and privacy for sharing the information. Here, the user and resources are more considered since more information is shared between them such as photos, videos, songs, etc,. and other information (such as photo tagging) where they can me exposed, since not all the users are aware of using the privacy options in the OSNs. There are more policies and specifications that are based on user-to-user relationship provides more security and privacy to the users.

In OSNs, user's access to the resources are based on the relationship that is between a user and other user connected through the network which is found to be the target in the graph representation of the social network. This relationship type which is based on the access control which refers to ReBAC (refered as Relationship based access control model) provides the relationship of the particular sequences or existences of the relationship and express the polices of access control on terms of

user-to-user relationship.

Consider some social network like "Google+" and "Facebook" provides some privacy options such as "private", "public", "friends list", "circles" and "friends of friends". These are some predefined options that are mostly used in the OSNs and provides privacy to the user groups. There are some researches who proposed some advanced model which is related to relationship based access control model such as [2],[4],[5],[7],[8],[9],[11],[12],[13],[14] can be given with multiple types of relationship based access control. Here [7],[8],[9] provides a decentralized security framework, Rule-based access control and enforcing access control over web based social network.

In this document, we provide a privacy and security for User-to User Relationship Access Control Model which gives the user to access others information in the depth of the relationship of that user. Here, In Facebook, consider there are three users Alice, Bob and John. Alice is a friend of Bob and John. But Bob and John are not friends. Here, Alice tries to hide Bob's information from John. For this Alice checks the relationship between Bob and John, If the relationship does not exist then Alice will hide Bob's information from John. This is done only if John tries to get Bob's information through Alice, then Alice will hide Bob from John. So that John cannot find Bob when he try searching in any place.

This document consist of some sections where Section 1 will give the related work or concept that is related or concept refered to any other journal papers. The next Section 2 is about the project that gives detailed explanation with the example. Section 3 gives the Algorithm that is explained in our project . The Section 4 gives Conclusion and Future Enhancement.

II. RELATED WORK:

This section gives related works that are refered to our paper and consist of some more information.

A. User Defined Privacy:

In this paper, we use OSNs where the users trust the resources that are to be used for sharing the information. Persona an OSN [3] describes the user-defined privacy which uses attribute-based encryption technique for hiding the data that user wants to hide his/her own information from the other user. This paper defines the access control model by which the information is more secured from the other user. The [3] paper uses a cryptographic technique which is based on attributes that need to be hidden from the other user. Here, Facebook has Persona's application where it is used to hide any particular type of information in the profile.

B. Social Network Polices:

In [1] paper, is a survey related paper ,defines the social network sites that are attracting the attention of the researchers. This survey paper is refered to our project since all the definitions such as about social network sites where each users are allowed to (1)get a public profile within a model,(2)share any type of information to the groups of users ,(3)can hide or block the users who are not required.

The profile visibility is different for different sites. For example, Friendster provides the user profile that are done by the servers and they are visible to anyone that, that user must not have any necessary to have an account in that particular site.

Conversely, LinkedIn has as access control, that the user to view another users' account must have an account in LinkedIn or he/she has to be paid. Some sites similar to MySpace ,makes a control over the profile by which the other user must view their own profile or not. This can be given with some options such as "friends only" and similar options. The Graphical and Structural variations among users by visibility and access are the only way that each sites in SNSs(Social Network Sites) are differentiated from them.

Generally, the privacy in the Online Social Network is not been maintained, Since in many ways the information from one user is taken by others. In some places, many users' Facebook account has been hacked or their information has been taken, and some other unrelated information are being posted in their profile by this unauthorized access of the user's profile. This should be prevented in some way that the unknown user must able to edit or change the content of particular user and should not misuse their account in any way. Hers the Facebook also provides some options like
"friends only","friends of friends","private" ,"public ", these options are provided to protect or secure the useres' profile from others user. To secure one's information or profile from other user who are common to a single user, he can be able to hide one's information or profile from other which is discussed in our paper. For example, if Bob has two friends like his father and his school mate in his friend list. Bob tried to hide his friend name from the friend list where his father cannot see his friends name in Bob's friend list this is done to hide Bob's friend viewing from his father. In other survey related paper like [15] gives detailed study over the social network how it meets the social science. Here the author Sergey Chernov ,tells that the social network can also be implemented through social science which can be in terms of sociology , political science, economics and psychology. Each term gives detailed description over the social network, that are mostly used by the users in all over the world.

C. Access Control Model For Osns:

In [16] the author gives the idea that, the relationship between each user and the resource gives the existence of the user activities and also controls the user activity. By now the OSNs are more used in all the ways but they are generally used in

tracking the relationship between the user and the resource owner that are used. Fong and Siahaan [13] gives the relationship based access control policies that provides privacy policy that keeps information more secured and each polices provide secure the data or any type information.

In [17] the author Aditi and Jyoti provide some Survey on User to User relationship based access control in which each user and the resource are linked together for better communication and more information are shared and then the polices are activated since more number of users are accessing the network at the same time. The network flow for the portion of the Social Network is given below.

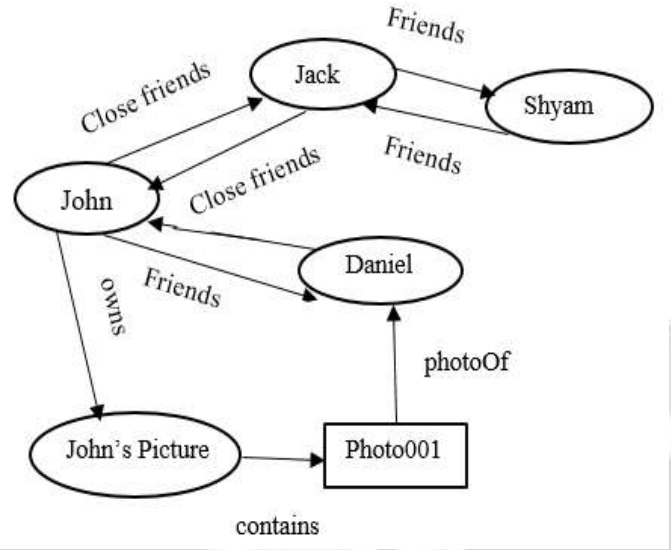
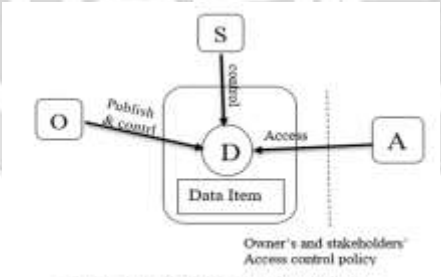


Fig.1.1 Portion of Social Network

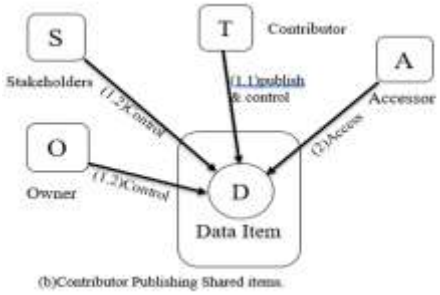
In the given figure 1.1, the process of sharing one's photo as a portion of the social network is given. Here, John is a close friend of Jack where John is just a distant friend of Daniel. Shyam is a friend of Jack. Here, John tires to share his photo only with his friend Daniel where John has his own view of showing his photo to his friends. This gives privacy over information shared between the friends. Shyam is just a friend of Jack and John only be accessing its own information from sharing from their information. Here, Jack cannot view John's photo since he has privacy that only Daniel can only view his picture.

In [18] the author Jorgensen provides a framework which designs the multiparty access control for data sharing.

Here sharing the data between the user to user is simple since privacy can be maintained. But the information between the multiple user cannot be or complex to maintain. So in our paper we defined how to secure and maintain privacy while large amount of information is shared in the social network. This gives the idea that any number user can share the information and that will be maintained and secured



(a)A multiple stakeholders with their shared items



(b)Contributor Publishing Shared items

Fig 1.2 Multiparty Authorization in OSNs Scenarios.

In the Fig1.2 (a) gives the scenario of the sharing of data through one OSN to another OSNs. Here Stakeholders acts as a major part where it is used to share a larger amount of data that can be seen or viewed by other networks when the shared network gives permission to access their own network. The next diagram (b)gives the description of the multiple stakeholders share their information to Contributors where there are multiple stakeholders to communicate.

For example, When Ram view's a post in Raj's space and selects to share this post with his friends, the post will be in turn posted in his space and he can specify a access control policies to authorize his friends to view it or not. In this case, Ram is a disseminator of the post. Since Ram may work on a weaker control by applying the options like viewing the post to everyone, the initial control of the post should be with, preventing the leakage of information of the post. This is to prevent the leakage of information of the post by any other friends if Ram sets the privacy option to public. Prevention is better than cure is a proverb which is necessary in all places. Here if we prevent for accessing of our information by unauthorized users can able solve more future problems that araises in future.

III. PROPOSED MODEL.

In this paper , we propose a model that defines a basic User-to-User relationship model that describes the use of Access Control model which gives privacy for sharing the information. Here, for an example consider three users Alice Bob and John. Alice is friend of Bob and John, but Bob and John does not know each other and John tires to take the information of Bob through Alice. Here, Alice comes to know that John is trying to take Bob's information then, Alice will hide Bob's profile from John., this is our paper, where privacy is maintained from one user to another.

Here Alice will check if there is any relationship between the two users Bob and John if the relationship does not exist the Alice can hide Bob from John. This is represented in a pictorial representation in the figure 1.3.

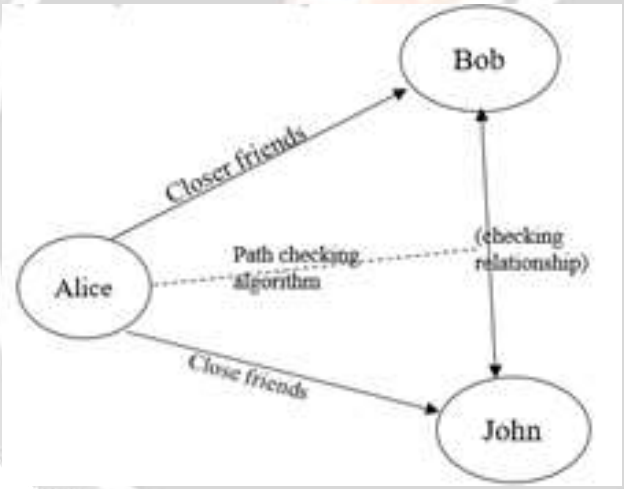


Fig 1.3 Checking the existence of relationship.

In the Figure 1.3 the existence of relationship is checked whether the two friends Bob and John are friends or not. If they are friends there in no need to apply the privacy between them and if they are not known then privacy should be maintained between the known and the unknown users between them.

For providing this privacy we include an algorithm called extended access evaluation algorithm for hiding a particular friend from another friend. Previously in [19] only single user access control is being maintained such as privacy between user to user relationship comes with hide any particular information from the other user. This explain only a part where only one user can hide his own information from other through the options like "private" , "public" , "friends" , "friends of friends" and so on.

The system architecture of the paper will be given below in the figure 1.4.

In the fig 1.4, the architecture of the system model is given. Here, there are 3 users(there can be multiple number of users since it is a architecture only 3 users are used here, it is based on particular user) where they need to register into the site.

Here we take an application similar to Facebook in which these users are registered to that site before they are used in the process. Then after registering into the Site the user will login into the site for performing certain operation or sharing any information. Here consider some four friends like Asha, Anu, Anil and Akash. Here Asha is close friend of Anu, Anil and Akash, but these three are not known to each other.

Here Anil tires to take the information of Anu without the knowledge of Asha, since she is the common friend. Once Asha comes to know about this through any notification Asha will hide Anu from Akash. Here, before hiding Anu from Akash, Asha will find if there is any relationship between Anu and Akash, if the relationship does not exist then she will hide Anu from Akash.

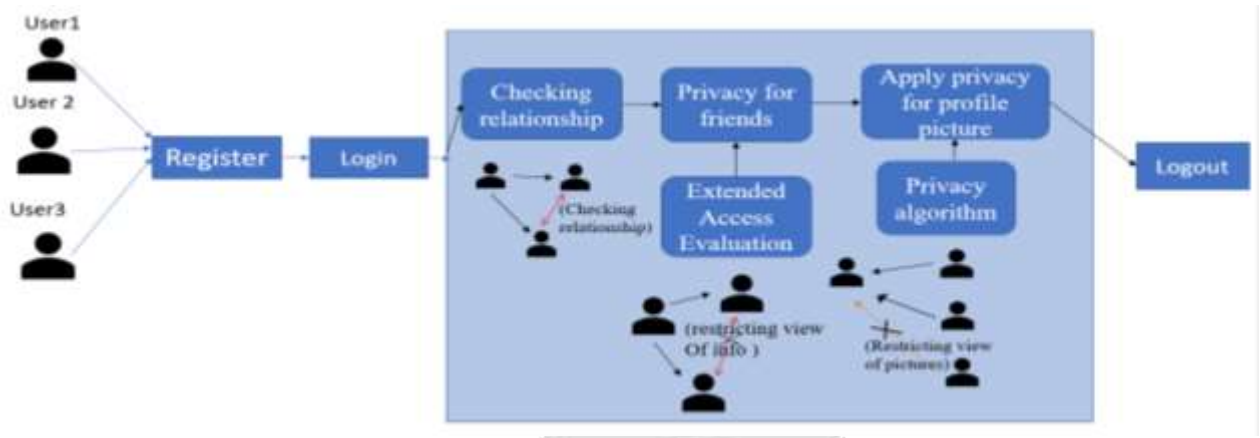


Fig 1.4 System Architecture.

Here Asha can hide not only Anu's information but also, she can hide n number of people from her friend list, where n is the number of people in her friend list. Additionally we can protect our profile picture from within our friend list. Here if Asha has 10 friends and she tries to hide her profile picture for only 4 friends and rest of them will view her original profile picture. She will group that 4 friends with one name and she will protect her profile picture with her duplicate picture, that
4 friends will be viewing only her duplicate picture and others will be viewed with her original picture. The pictorial representation will be given as below.

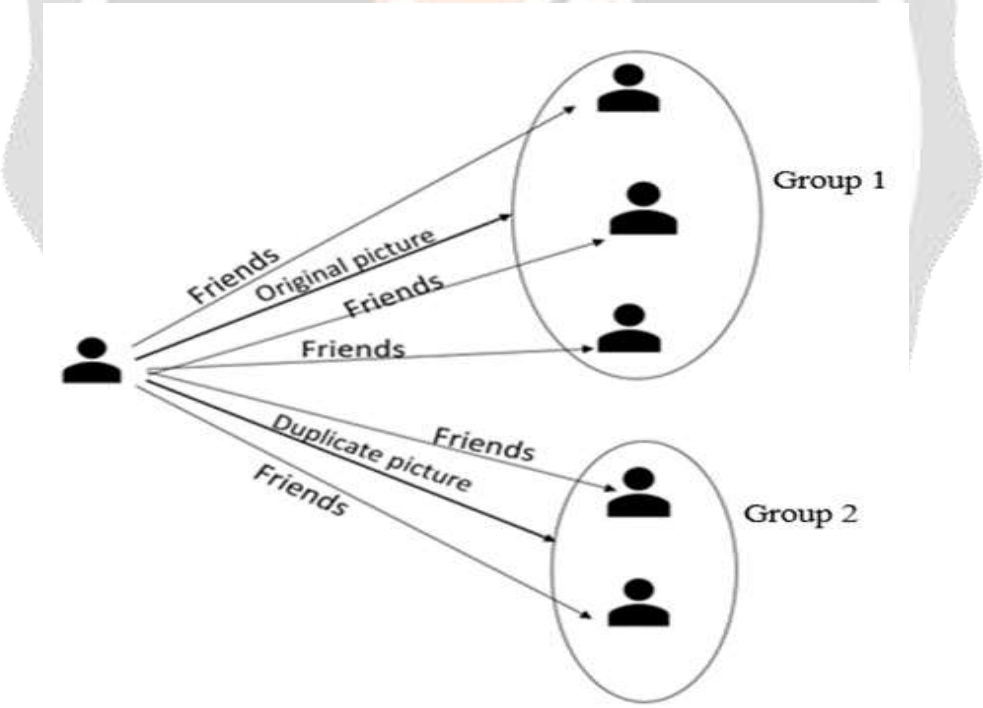


Fig 1.5 Profile Picture Privacy Among Friends.

In the Figure 1.5, there are two groups in which two group people are friend of a single user. Here the user will view his/her original profile picture for group 1 and duplicate profile picture for group 2. For this Privacy preservation algorithm is used for hiding the profile picture from one person to another person.

IV. ALGORITHM:

In this paper , we define a algorithm which is used for providing the privacy for the users. For this we use an extended access evaluation algorithm along with path checking algorithm is also used.

These algorithm is shown in the below table.

Table 1.1. Extended Access Evaluation Algorithm.

1: (Policy Collecting Phase)
2: **If** Target = Ut **Then**
3: Accessing User Policy Ua's Policy For Action, Target User Policy Ut's Policy For Action1, Specify Policies System's Policy For Action
4: **Else**
5: Accessing User Policy Ua's Policy For Action, Target Resource Policy Rt's Policy For Action1, SP System's Policy For Action; (R:typename; R:typevalue)
6: (Policy Evaluation Phase)
7: **For All** Policy In Accessing User Policy, Target User Policy/ Target Resource Policy And Specify Policies **Do**
8: Extract Graph Rules (Start, Path Rule) From Policy
9: **For All** Graph Rule Extracted **Do**
10: Determine The Evaluating Node Which Is The Other User Involved In Access
11:(Path Checking Phase)
12: Extract Path Rule From Graph Rule
13: Extract Each Path Spec Path, Hopcount From Path Rule
14: Path-check Each Path Spec
15: Set The Access Permission Over The Existing Path
16: Configure The User Profile Privacy
17: Evaluate The Combined Result Based On Conjunctive Or Disjunctive Connectives Between Path Specs And Negation On Individual Path Specs
18: Compose The Final Result From The Result Of Each Policy

In the given algorithm , there are three types of phases. One is Policy Collecting Phase, where the policy in which the user want to collect from the other user who he needs to hide from his friend and after collecting the required information the user will hide the privacy through the next phase called Policy Evaluation Phase. Here the collected policy are evaluated and then the process is taken in the account with all the policy like User Access Control policy, Target User Policy and Target Resource Policy. These policies are collected before they are used in the process and after the information are collected the policy evaluation phase starts by checking the policy collected are correct and if the collected policy are not correct then the process of verifying the policy evaluation phase fails. This phase the policy are checked and then the target and the destination are fixed that who need to hide whose profile from whom is define here. The hopcount is the numerical value which gives the value of number of users or friends available in the friend list. By the hopcount value the process will be generated by which the policy and the user who must be hidden will be given by extracting the other values in the process.

Here path checking algorithm is used for searching or finding the path that need to be performed in the process. So each path by which who is friend of whom and if there is any relationship between them or not , all these are checked and the verified by the path checking evaluation phase. Here the value of hopcount is used for further path checking and evaluation of the process.

If the result is true then the process is done (i.e) one user is hidden from the other user. If the result is false then there is a relationship between those two users. At that time the evaluation cannot be performed.

V. CONCLUSION

In this paper, we proposed a user-to-user relationship model and a policy specification for protecting the data from the unknown user. We provided a DFS-based path checking algorithm and analyzing the complexity of the algorithm. We then perform evaluation results.

We also believe that the proposed model in this paper provides a solid foundation for more advanced ReBAC solutions in future.

VI. REFERENCE.

[1] D.M.boyd and N.B.Ellison, "*Social Network Sites:Definition,history and scholarship"* J.Compute. Meditated Commun., vol. 13, no. 1, ppt. 210-230,2007.
[2] G. Burns, P.W.Fong, I. Siahaan and M.Huth, "*Relationship based access control : Its expression and enforcement through hybrid logic,"* in Proc. Second CODASPY,2012, pp. 117-124.

[3] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "*Persona: An online social network with user defined privacy"* ACM SIGCOMM Compute. Commum. Rev., vol. 39, no. 4,pp. 135-146,2009.
[4] B. Carminati and E. Ferrari , R. Heatherly , M. Kantharcioglu and B. Thuraisingham, "*A semantic wed-based framework for social network access control "* In Proc. 14th ACM SACMAT, 2009, pp. 177-186.
[5] B. Carminati and E. Ferrari , R. Heatherly , M. Kantharcioglu and B. Thuraisingham,(2011*)."Semantic web-based social network access contorl"*. Comput. Secure., vol. 30, no. 2C3.
[6] C. Gates, *"Access Control requirements for web 2.0 security and privacy,"* IEEE web 2.0 , 2007.
[7] B. Carminati and E. Ferrari , and A. Perego, *"Rule based access control for social network "* in Proc. Move Meaningful Internet Syst. 2006 OTM 2006 workshop, 2006, pp. 1734-1744.
[8] B. Carminati and E. Ferrari , and A. Perego*,"A decentralized security framework for web-based social network.",*. Int. Journal of Info. Security and privacy vol.2 , no. 4, 2008.
[9] B. Carminati and E. Ferrari , and A. Perego,"*Enforcing access control web-based social networks".* ACM TRANS. Inf. Syst. Secur., vol. 13, no. 1, 2009.
[10] H.Gao, J. Hu, T. Huang, J. Wang and Y. Chen, "*Security issues in online social networks ,"* IEEE internet Comput.,vol. 15, no. 4, pp. 56-63, July./August 2011.
[11] P. W. Fong , *"Relationship based access control; protection model and policy language,"* In Proc. First CODASPY, 2011, pp. 191-202.
[12] P.W. Fong, M. Anwar, and Z. Zhao,"*A privacy preservation model for Facebook style and social network system"*, In Proc. Comput. Secur.- ESORICS, 2009, pp. 303-320.
[13] P. W. Fong and I. Siahaan , "*Relationshio based assecc control policies and their policy languages*", In Proc. 16th SACMAT, 2011, pp. 51-60.
[14] S. R. Kruk, S. Grzonkowsai, A. Gzella, T.Woroniecki, and H. C. Choi ,"*D-FOAF: Distributed identity management with access rights delegation"* In THE semantic web-ASWC 2006, Springer, 2006, pp. 140-154.
[15] Sergey Chernov "*Social Networks Meet Social Science ",* Proceeding of the 16th All- Russian Conference- RCDL-2014, Dubna, Russia, October, 13-16, 2014.
[16] Y. Chaeng, J. Park and R. Sandhu, "*A user to user relationship based access control model for online social networks,"* In Proc, 26th data APPL. Secur. Privacy. 2012, pp. 8-24.
[17] Aditi V Bhadke and Jyoti Raghatwan, "*Survey on User-to-User Relationship based Access control for OSNs"*

[18] H. Hu and G. J. Ahn;"*Multiparty authorization framework for data sharing in online social network."* In Proc,. 25th data appl. Secur. Privacy., 2011,pp. 29-43.
[19] Yuan Chen, Jaehong Park, and Sandhu*,"An Access Control Model for online social network using user-to-user relaionships,"* vol 13, no. 4, July/August 2016.,pp 424-436.