ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Multi-Party Privacy Conflict Detection and Resolution in Social Media

Tanuja Vilas Patare, Prof.N.G.Pardeshi

Department of Computer Engineering, SRES, Sanjivani College of Engineering , Kopargaon, Maharashtra, India

Department of Computer Engineering, SRES, Sanjivani College of Engineering , Kopargaon, Maharashtra, India

ABSTRACT-OSN's got huge growth in recent years for connecting people and sharing data. It mostly becomes a platform of gaining private and sensitive data about individuals.Things shared may influence more than one client's security, e.g., photographs that show to different users, and so forth. A current standard Social Media framework makes clients not able to properly control to whom these things are really shared or not. Here sometimes users are unaware about their actions on a social media. Computational mechanisms that are able to merge the privacy preferences of multiple users into a single policy for an item can help to solve this problem. However, merging multiple users' privacy preferences is not an easy task, because privacy preferences may conflict, and conflicts resolution is needed. System needs methods in order to propose solutions that can be acceptable by all of the users affected by the item to be shared. Current approaches to solve this problem are either too demanding or only consider fixed ways of aggregating privacy preferences. In this paper, system propose the first computational mechanism to resolve conflicts for multi-party privacy management in Social Media that is able to modelling the concessions that users make to reach a solution to the conflicts. System also present results of a user study in which proposed mechanismperformed better than other existing approaches, in terms of how many times each approach matched users' behaviour. System considers users' willingness about granting or denying the access when solving conflicts in this domain. In particular, system also produces the result for sharing and privacy loss ratio to find out the effectiveness of the proposed mechanism. As Future work, system can explore the other factors that could match user behavior, like for instance if concessions may be influenced by previous negotiations with the same negotiating users or the relationships between negotiators themselves.

KEYWORDS: Privacy policy**,** Conflicts,Multi-party**,** Negotiation.

I. INTRODUCTION

Now a day's no of items upload by multiple users on online social media and users can set their privacy preferences for that items .But social media only allows uploader to set his privacy policy for that item i.e. who can have access to the item. This is may lead to privacy violations that other users who affected by that item cant set privacy preferences for it. For example photo in which multiple users are included and one of the user wants to upload that photo on social media (uploader) then only he having rights about to whom he wants to share that photo. But here the other users in that photo may have privacy issues regarding this situation. The existing approach uses manual user negotiation to solve this problem i.e. email, SMSs, phone calls etc. But this approaches require more time to deal with situation manually because there are multiple uploader and accessor are present on social media. In this paper system introduces a new approach to deal with these privacy issues. Here system considering all users individual privacy preferences and identify at least two policies that having contradictory decisions about granting/denying access for that particular item i.e. privacy conflict. System provides a conflict solution by modelling access control in such a way that all users involved in that uploading item accept that solution and ensure about their privacy.Negotiating users have their own individual privacy preferences about the item that is, to whom of their online friends they would like to share the item. Here system assume users to specify their individual privacy preferences using group based access control, which is now a days mainstream in Social Media (e.g., Facebook lists or Google+ circles).Here other access control approaches for Social Media also be used in conjunction with proposed mechanism for ex. relationship based access control or (semi)automated approaches. Proposed approach does not necessarily need users to specify their individual privacy preferences for each andevery item separately, they could also specify the same preferences for collections or of the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

items for convenience according to the access control model being used-e.g., Facebook users can specify preferences for a whole photo album at once. Proposed system allow users to define their own groups, to organise their online friends.

1.1. Background

a. Data Co-Ownership in SNs

System present the co-ownership in SNSs and discuss how to detect co-ownership of detain a semi-automated manner. In SNSs, users post data on their profiles, this data is usually considered owned by the profile owner. The profile owner has to take the responsibility of managing the access of the posted data content. However, data posted on a user's profile often conveys content not belonging only to the profile's owner. For example, documents can be belong to multiple individuals that is several users may appear in a same picture, and the same applies to other media content, such as videos. If Alice posts a document in her profile which belongs also to Bob, she is in charge of setting the privacy policy for the document, regardless of whether Bob is happy with her policy or not. These simple observations naturally lead to the idea of supporting co-ownership (or stakeholders) in SNS, to indicate the set of users who are owners of a piece of data, regardless of where (i.e., in which user's profile) this data has been originally posted.Assume a finite set of users U, where a finite subset of negotiating users N, the users deciding the access permissions for their sharing data, whether they should grant a finite subset of target users T access to a particular co-owned item. For instance, Alice and Bob(negotiating users)negotiate about whether they should grant Charlie (target user) access to a photo of Alice and Bob together.

1.2Motivation

For many social networking sites users are actively encouraged to upload and share content and information, often with strangers. This has led to number of incidents where personal data available on a social networking site and get exploited for uses other than it was originally intended. In several recent cases, people have lost their jobs due to the posting of inappropriate comments and photographs on Facebook .To safeguard users' privacy online, privacy protection mechanisms are needed. These mechanisms limit the scope for attacks on user privacy by ensuring that accesses to a user's data are authorized by the user. Existing privacy protection mechanisms enable users to specify policies for their data. They do not support cases where disclosure of data affects several individuals.

1.3. Aim and objective

Aim: Our aim is to find out the privacy violations for sharing item on a social media and solves these issues with automated conflict resolved policy for multi-party privacy management.

Objective :

1. To provide individual privacy policy to all users.
2. To provide privacy conflict detection.
3. To provide automated privacy conflicts resolution.

II. LITERATURE SURVEY

Unparalleled development in the use of Online Social Networks. For instance, Facebook, LinkedIn and twitter to illustrative informal community destinations, guarantees that it has more than 600 million dynamic clients and morethan 40 billion sections of shared substance of all month, counting site url joins, news articles, stories blog entries, individual notes and photograph collections. Due to this development many privacy issues occurs in front of the social media user. This section discusses the different work and issues handled until now. In [1], author shows the issue of community authorization of protection approaches on shared information by utilizing diversion hypothesis. It proposes an answer that offers computerized approaches to share pictures in view of an augmented thought of substance proprietorship. Expanding upon the Clarke-Tax instrument, we depict a straightforward component that advances honesty, and that prizes clients who advance co-proprietorship. We incorporate our plan with deduction procedures that free the clients from the weight of physically selecting security inclinations for every photo.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

To the best of our insight this is the first run through such an insurance component forSocial Networking has been proposed. It likewise demonstrates a proof-of-idea application, which it executed with regards to Facebook, one of today's most mainstream informal organizations. It demonstrates that supporting these kinds of arrangements is not likewise doable, but rather can be executed through an insignificant increment in overhead to end-clients. In [2], author proposes a security, person to person communication, informal communities permit clients to confine access to their own information, there is as of now no tool to implement security worries over data transferred by different clients. As gathering photographs and stories are shared by loved ones, individual protection goes past the circumspection of what a client transfers about him and turns into an issue of what each system member uncovers. It analyses how the absence of joint protection controls over substance can unintentionally uncover delicate data about a client including inclinations, connections, discussions, and photographs. In particular, we investigate Facebook to recognize situations where clashing security settings between companions will uncover data that no less than one client proposed stay private. The uncovered data in this way, it exhibit how a client's private properties can be construed fromjust being recorded as a companion or specified in a story. To alleviate this risk, it indicates how Facebook's securitymodel can be adjusted to uphold multi-party protection. It displays a proof of idea application incorporated with Facebook that naturally guarantees commonly adequate protection limitations are implemented on gathering content.

In [3], author offers interesting means for virtual social communications and data sharing additionally raise various security and protection issues. In spite of the fact that OSNs permit a single client to administer access to her/his information, they right now don't give any tool to authorize security worries over information connected with various clients, remaining protection infringement to a great extent uncertain and prompting the potential divulgence of data that no less than one client proposed to keep private. It proposes a way to deal with empower community oriented protection administration of shared information in OSNs. Specifically, it gives a deliberate component to distinguish and resolve protection clashes for cooperative information sharing. The contention determination shows a trade-offs between protection assurance and information sharing by measuring security hazard and sharing misfortune. It talks about a proof-of-idea model usage of our approach as a component of an application in Facebook and give framework assessment and ease of use investigation of our procedure.

In [4], author proposes a way to deal with empower the security of imparted information related to numerous clients in OSNs. It gets to control model to catch multiparty approval prerequisites, alongside a multiparty arrangement determination plot and a strategy requirement tool. It shows a legitimate representation of our get to control demonstrate that permits us to influence the elements of existing rationale solvers to perform different investigation errands on our model. We additionally examine a proof-of-idea model of our approach as a component of an application in Facebook and give convenience study and framework assessment of our strategy.

In [5], author shows the absence of multi-gathering security administration bolster in current standard Social Media frameworks makes clients not able to properly control to whom these things are really shared or not. Computational tool that can consolidate the security inclinations of different clients into a solitary strategy for a thing can take care of this issue. Be that as it may, consolidating numerous clients' security inclinations is not a simple undertaking, since protection inclinations may struggle, so strategies to determine clashes are required. In addition, these techniques need to consider how clients' would really achieve an assertion about an answer for the contention with a specific end goal to propose arrangements that can be adequate by the majority of the clients influenced by the thing to be shared. Current methodologies are either excessively requesting or just consider settled methods for amassing protection inclinations. It propose the principal computational instrument to determine clashes for multi-party protection administration in Web based social networking that can adjust to various circumstances by demonstrating the concessions that clients make to achieve an answer for the conflicts. It additionally shows consequences of a client concentrate on in which the proposed component beat other existing methodologies regarding how often every approach coordinated clients' conduct.

III. EXISTING SYSTEM AND DISADVANTAGE

The popular existing OSNs such as Facebook, Myspace, Orkut, Twitter, and Google+ continuously updating their functionality and privacy setting. Facebook provides the most fine-grained access control policies to preserve users

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

privacy, but it can potentially leak users sensitive information as it considers only owner's privacy preferences.Unlike Facebook and MySpace, Orkut does not offer any settings to preserve users friend-lists (i.e., anyone can collect them). Twitter and Google+ adapt directional friend-lists such that a user has two independent friend-lists: followers and followings. As a result, they can define independent publication policies for their own friend-lists. However, these services allow users to display not only their followings but also followers, which causes a policy conflict.The comparison of the privacy policy conflicts in different OSNs is as shown in following Table 1.1.

OSNs	Friend	Stream	Image	Group
Facebook	+	+	-	+
MySpace	+	-	+	*
Twitter	+	-	+	*
Google+	+	-	-	*

+: Sensitive information can leak, -: Sensitive information cannot leak, *: Not implemented.

Disadvantages:

1. For facebook sensitive information can leak through Friendlist, stream and group.
2. For Myspace,Twitter sensitive information can leak through Friendlist and image.Both are not implemented for group.
3. For orkut sensitive information cannot leak through stream only.
4. Google+ provides protection for stream and image but not for Friendlist.
5. Existing approaches having a risk of privacy loss
6. User have to negotiate manually to solve privacy issues.

IV. PROPOSED SYSTEM ARCHITECTURE AND ADVANTAGES

It is asocial networking site with functionalities where user can utilize the application,creates social connection and share data. The social media have multiple no of users. The system proposes mainly two types of users negotiating and target user. Firstly negotiating users is a set of users who co-own an item. One of them wants to upload an item and other users become affected users who involved in that item.Second one is targeted users set, to who item will be shared or they having access to the item based on negotiating user's privacy policy. Figure shows the proposed system architecture.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

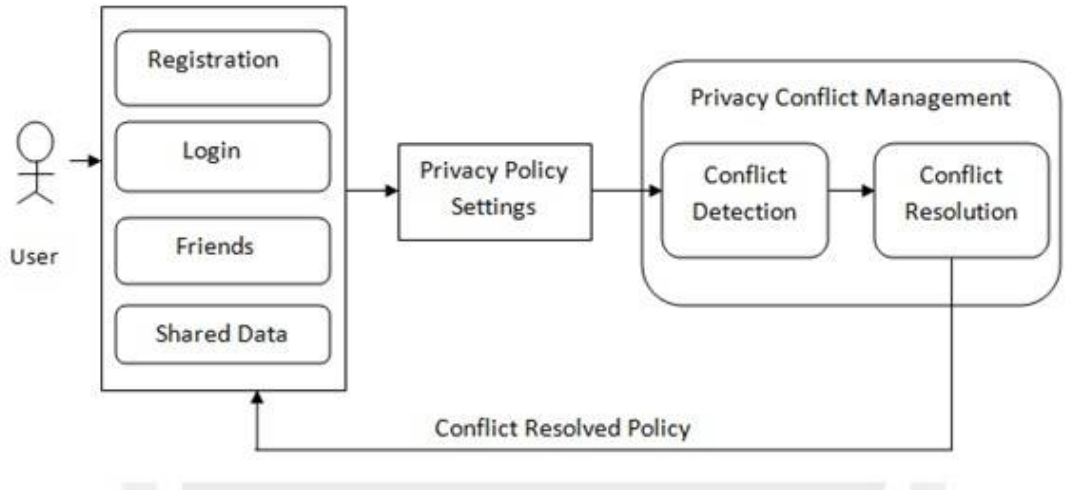


Fig01 : Proposed system mechanism

a. Registration:

Every user will have a registration phase where user have to full fill the required fields like their personal details with name, email id as a username and password with valid specifications, address, mobile no and user have to upload profile photo. Then only they can have access to the system.

b. Login:

Only the user with valid credentials can enter into the system. Their credentials will be verified from the server side and every user will be validated during login to maintain the genuineness of the user.

c. Friends:

Login user can search for friends and send friend request to them, to make online connections. Here user can accept or reject the friend request. User can have their own friend list by defining own groups.

d. Sharing data:

User can share data publically or privately. To share data privately user have to set their privacy access permission for item.

e. Privacy policy settings:

The access permissions privacy policy is either granting or denying access for particular item. User can individually grant or deny access for his/her friend list in a defined group. For grant access permission friends can view the message and friends can't view the message if access permission is denied. For co-own item negotiating user have to set their privacy preferences individually.

f. Conflict detection:

* Privacy Conflict: For co-own item users set their privacy policies, if it includes the contradictory decisions the it will become a privacy conflict.

- The admin inspects all the individual privacy policies for the same item.
- It looks at whether individual privacy policies contain contradictory decisions for the same target user.
- If conflicts are not found user can share images with their privacy preferences.
- If conflicts are found the item is not shared preventively and it will go to the resolution phase.

g. Conflict Resolution:

In order to find out a solution to the conflict that can be acceptable by all negotiating users, system have to consider following factors:

1. Relationship between each negotiating user with each target user known as "Tie-Strength".

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

*τ(a , b)= tie strength assigned for each pair. where a will be a negotiating user and b will be the target user. δ is the maximum positive integer value in tie strength that uses 6 levels of tie strength:

0= no relationship
1= acquaintance
2= distant friend
3= friend
4= close friend
5= best friend

2. Importance of conflict user to the negotiating user.
3. The concession rules to match the behaviour of user,so that it will resolve conflicts automatically.

Advantages:

- Propose system detect and solves privacy violations automatically, in such a way that it provides following advantages.
  - To provide individual privacy policy settings to all users , for sharing data.
  - It minimizing the risk of disclosure of sensitive data.
  - It resolves privacy conflicts automatically so that users need not to negotiate manually.
  - For minimizing the burden on the user to resolve multi-party privacy conflicts.
  - It reduces sharing as well as privacy loss.

V. MATHEMATICAL MODELLING

Mathematical model is a description of a system using mathematical concepts and language.When solving problems we need to analyse the difficulty level of our problem. There are three types of classes i.e. P Class, NP-hard Class and NP-Complete Class.Here Proposed system problem is NP complete.

Class NP is the class of decision problems that can be solved by non deterministic polynomial algorithm. This class of problems is called non deterministic polynomial.

1) Set Theory: A set theory concept is used to represent the mathematical model for the system,which consist of different sets for input,process,rule and output.

Let,
S = {I, P,R,O}
Where,
S: System
I: Set of inputs
P: Set of processes
R: Rules or constraints
O: Set of outputs/Final output
*I = {i1; i2}
Where,
i1: Authentication.
i2: Privacy Policies.

*P = {p1; p2; p3; p4; p5}
Where,
p1:Registration.
p2:Log In.
p3:File Sharing.
p4:Conflict Detection.
p5:Conflict Resolution.

*R = {r1}
Where,

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

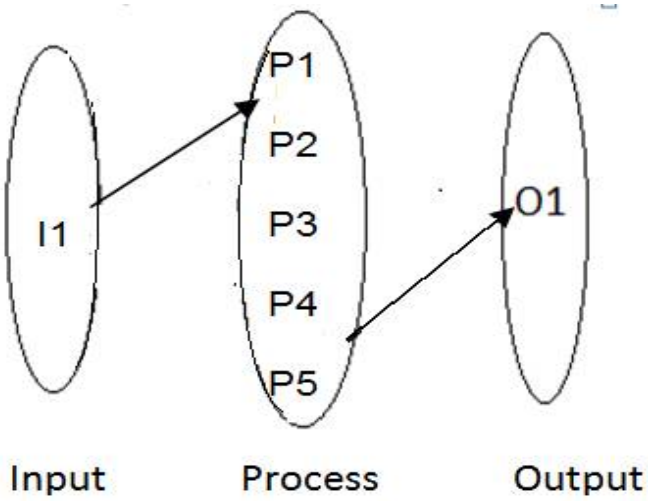
(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

r1:Only valid user can log in into system.

* O = {o1,o2}
Where,
o1: Detected Conflict
o2: Conflict Resolved Policy.
2) Venn Diagram: Venn diagram represents the interaction between different processes along with input and output. Figure shows the mapping of input, process and output.



VI. ALGORITHM USED

1) Conflict detection:
Input: Negotiating user, target users and privacy policies
output: Conflict users
1 .foreach negotiating_users do
2. foreach target_users do
3. action_vector = 0 //denying access
4. foreach group do
5. if user=target_user then
6. action_vector = 1 //granting access
7. end if
8. end for
9 .end for
10. foreach user do
11. action_vector = action_vector
12. end for
13. end for
14. Conflict = Ø
15 .foreach target_user do
16. Take negotiating_user
17. foreach negotiating_user do
18. if action_vector ≠ action_vector then
19. Conflict = Conflict of target_user
20. end if

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

21. end for
22. end for

2)Conflict resolution:

2.1. Tie strength between negotiating and target user:

TS = {Sum of all user priorities in a group/ Total no of members in a group}

2.2. Importance of Conflict User for negotiating user:

IC =| Tie_Strength – Priority set for conflict user |

2.3.Willingness to change action for conflict user:

W(N , C)= ½ { (|δ-IC| / δ+IC) + (|δ-TS| / δ+TS) }

2.4 Concession rules:

- I Do Not Mind (IDM) rule to accept the action that user would not mind much conceding and accepting that action for the conflicting target user.
  IF W(a,c) IS high THEN concede.
- I Understand (IU) rule where item is not detrimental to any of the users involved and there is any user for whom sharing is important.
  IF W(a,c) IS low ^ Va[c] = 1^
  ∃bЄ N; W (b,c) IS low ^ Vb[c] = 0
  THEN concede.

- No Concession (NC) rule for the other cases in which neither IDM nor IU applies, then the system estimates that a negotiating user would not concede.

IF W(a,c) IS low
^(Va[c] = 0_(∃bЄ N : W (b,c)IS low ^ Vb[c] = 0))
THEN do not concede.

Algorithm

Input: Conflict users,willingness
output: Resolved policy
1 foreach Conflicting_ userdo
2 if willingness(negotiating_user,conflicting_user)=high then
3 action_vector=modified_majority(privacy_policies,conflicting_user) //IDM rule
4 continue
5 end if
6 if willingness(negotiating_user,conflicting_user)=low then
7 if willingness(negotiating_user,conflicting_user)=low
andaction_vector≠ action_vector then
8 action_vector=0 //denying access
9 else
10 action_vector = 1 //granting access
11 end if
12 end if
13 end for

VII. EXPERIMENTAL SET UP

- Methodology of evaluation
  - We are implementing the system using Java with eclipse jee-luna-SR2-win32 and apache-tomcat-7.0.42. with JSP server serving java technologies.
  - Our System uses MySOL, a open source relational database management system that uses SQL for adding, managing and accessing content in a database.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

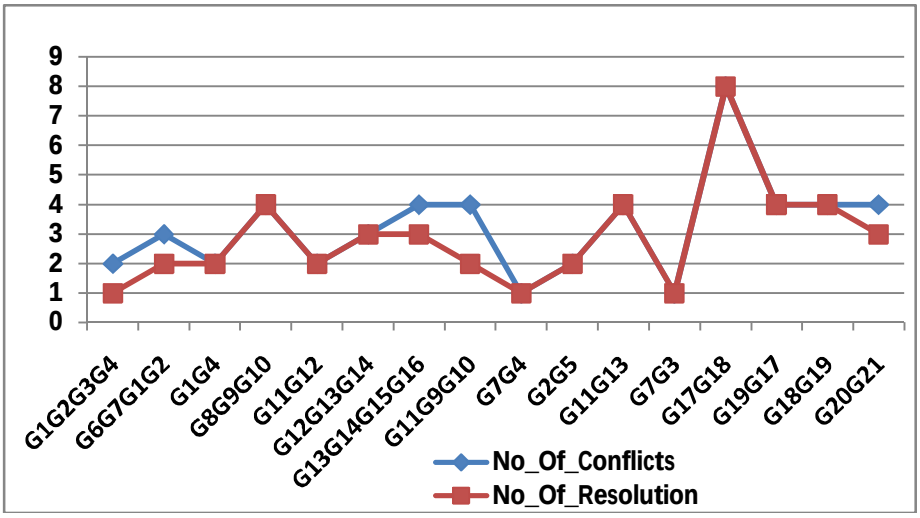
Vol. 6, Issue 6, June 2017

- The Microsoft Windows 7 is used as an operating system.

Consider system with total no of 100 users and 21 groups. Proposed system tested almost #52 instantiations and the result will be as follows:

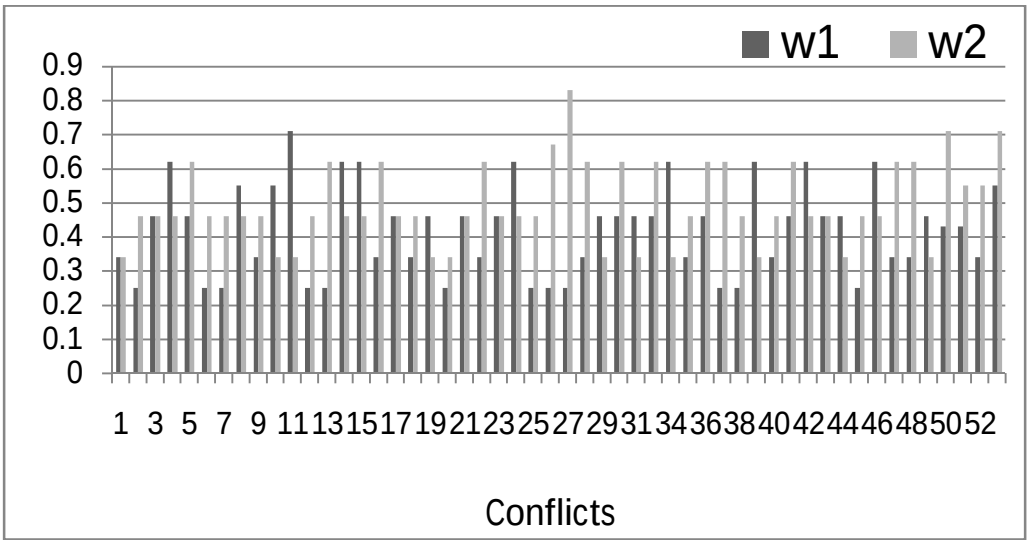
1. No of detected and resolved conflicts for groups:

Here 21 groups are involved in a user study, where 16 combinations of groups are present and for each of that system have detected and resolved conflicts. The occurrence of conflict is depends on a privacy policies set by negotiating user.For this user study system detects total no of 52 conflicts and differentiate them for each group.



2. Willingness to change action for each conflict detected by system:

Here system calculated the willingness of each negotiating user involved in each conflict. Willingness value decides whether negotiating user wants to change his/her preferred action for conflict user. Based on this value concession rules like IDM,IU,NC are applied to provide solution.



3. Number of Times AR Concession Rule Would Have Been Applied And existing approach matched with concession behaviour (Accuracy)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

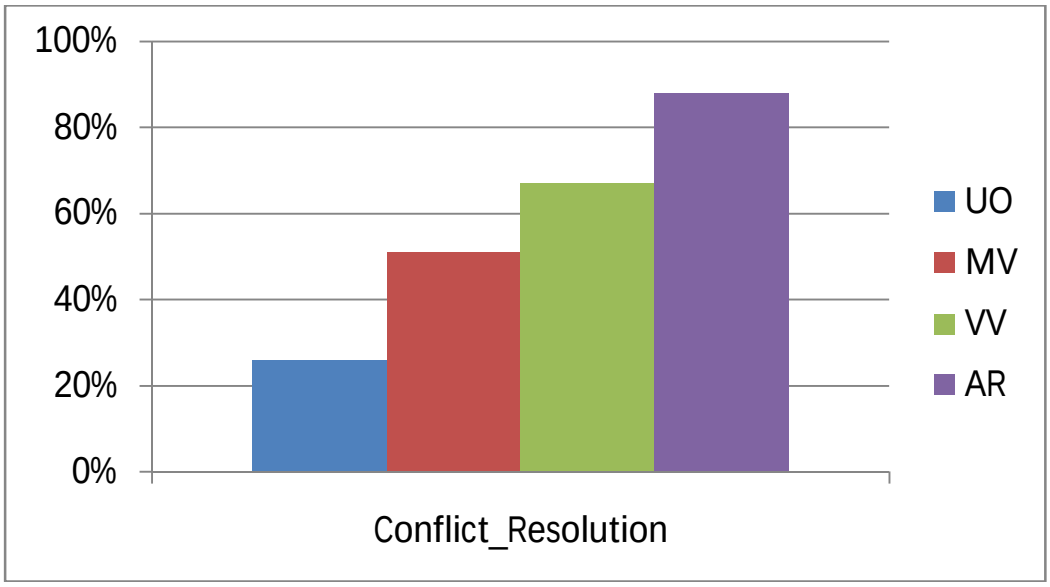
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

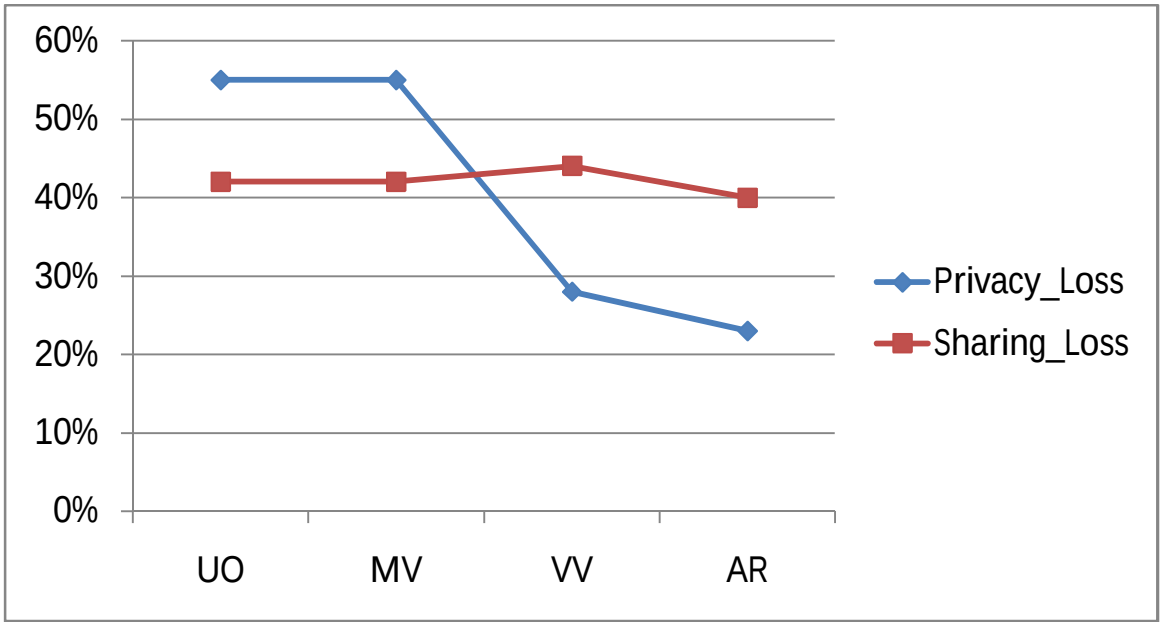
Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Apply existing approaches on a user study to find out how many conflicts get resolved with existing systems and percentage of times each approach (UO, MV, VV,) matched with concession behavior. Finally the proposed system's (AR) accuracy get compare with them. As shown in figure proposed system get better result than existing approaches.



4. Comparison between existing approach and proposed system using ratio of Privacy _ Loss and Sharing _ Loss
*Privacy _Loss: Here for AR 23% is a loss of privacy which is lower than other existing approaches.
* Sharing _ Loss: Here for AR 40% is a loss of sharing which is lower than other existing approaches.



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

VIII. CONCLUSION

In this way system introduces the new mechanism for conflict detection and conflict resolution techniques in Social Media. It reduces the amount of manual user interventions to achieve a satisfactory solution for all parties involved in multi-party privacy conflicts.This is a stepping stone towards more automated resolution of conflicts in multi-party privacy management.For future work it will find out the other factors that play role in solving privacy conflicts.

REFERENCES

[1] Jose M. Such,NataliaCriado, "Resolving Multi-Party Privacy Conflicts in Social Media",IEEE Transactions on Knowledge and Data Engineering, VOL. 28, NO. 7 July 2016.
[2] K. Thomas, C. Grier, and D. M. Nicol, "Unfriendly: Multi-party privacyrisks in social networks", by in Proc. 10th Int. Symp. Privacy Enhancing Technol., pp. 236–252,2010.
[3] J. M. Such, A. Espinosa, and A. Garcıa-Fornes, "A survey of privacy in multi- agent systems", Knowledge and Engineering Rev., vol. 29, no. 03 pp. 314–344, 2014.
[4] H.Hu, G. Ahn, and J. Jorgensen "Multiparty access control for online social networks: Model and mechanisms", IEEE Trans. Knowl. Data Eng., vol. 25, no. 7, pp. 1614–1627, July 2013.
[5] R. Wishart, D. Corapi, S. Marinovic, and M. Sloman "Collaborative privacy policy authoring in a social networking context",by in ProcIEEE Int. Symp. Policies Distrib. Syst. Netw., pp. 1–8, 2010.
[6] A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen, "We're in it together: Interpersonal management of disclosure in social network services",in Proc. SIGCHI Conf. Human Factors Comput.Syst., pp. 3217–3226, 2011.
[7] A. Besmer and H. Richter Lipford, "Moving beyond untagging: Photo privacy in a tagged world",in Proc. SIGCHI Conf. Human Factors ComputSyst.,pp. 1563–1572,2010.
[8] H. Hu, G.-J.Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks", in Proc. 27th Annu. Comput. Security Appl. Conf., pp. 103–112, 2011. [Online] Available: http://doi.acm.org/10.1145/2076732.2076747