User Intended Privacy Preserving Models in Online Social Networks

Amal Twinkle Mathew
PG scholar,
Department of CSE (PG)
Sri Ramakrishna Engineering College,
Coimbatore.

S. Saravana Kumar
Assistant Professor (Sr.Gr)
Department of IT,
Sri Ramakrishna Engineering College,
Coimbatore.

Karthikeyan. M
PG Scholar,
Department of CSE(PG),
Sri Ramakrishna Engineering College,
Coimbatore.

ABSTRACT

The proposed system introduces new social network privacy management models and it measures their human effects. Here it introduces a mechanism using clustering techniques which helps users to group their friends using policy management. Then it introduces new privacy management model which will give policies to other friends to find similar friends in the network. And thereby explored various ways that help users to find example friends. In addition, it will help to find privacy management models which can be further enhanced and also it helps to detect privacy sentiment of user. Assistant friend grouping will be done for effective friendship establishment. In a network user privacy will be maintained by setting privacy techniques. Privacy management models can be routinely customized to the privacy sentiment and done according to the needs of the user.

Keywords

OSN online social network, CNM clauset Newman’s moore

1. INTRODUCTION

Network administrator prevents and monitors the unauthorized access of data in network Security. Network security includes the authorization of access to data and also it helps to prevent the misuse, modification of data in a network. An ID and Password or some other authenticating information which is chosen by the user is used to access the information within their authority. Network Security will secure network as well as operations being done.

1.1 Overview of the Project

Social networking sites are increasingly used in this new era and its growth is tremendous. This internet and social networking sites are being part of the young generation. Not only there are many users online, there is also a tremendous amount of user profile and content online. There are almost 30 billion pieces of content being shared every month. Everyday new contents are being added and these contents are coupled with different number of users online and this will lead to challenge in privacy. There are various studies being done concerning privacy. There are various conclusions being found out. Now there are varying levels of privacy controls, depending on the online sites. Here some sites will reveal all the user profile data without the restriction and this will lead to loss of privacy. While in other sites they will reveal user profile only to trusted friends .Other studies includes privacy paradox , the relationship between individual privacy intentions to disclose their personal information and their actual behavior. These research concludes that it lacks informed privacy decisions . But to manage ones privacy is quite difficult.

1.2 Principle of Social Networking

Here we take facebook as the example in our because it is currently mostly used online social networking site. It can also be easily extended to other existing online social networking platforms. To provide various services, these sites uses name, birthday, interests of different users . it can also take different profile attributes of a user’s friends to make it more complicated.

Here users can select particular pieces of profile attributes they want to share, when their friends use different applications . at the same time users who are using the application will also control the information which are private to them. This means that when an application access the profile of a friend then it will have to gain control over both friend as well as user over the profile attributes. It also shows a profile sharing pattern in various situations.

1.2.1 OSN Security

Data sharing patterns coupled with multiparty authorization in OSNs are identified. Social Networking Sites such as Face book, Google+, and Twitter will help the people to share private and public information and this will help to maintain social connections with friends, colleagues etc. now there is a vast growth in the application of OSN. So the security of the data has been a threat and access control has become the central feature of OSN . Social applications on current OSN platforms can also consume the profile attributes of a user’s friends. In this case, users can select particular pieces of profile attributes.

1.3 Problem Statement

Human Effects is major problem predicted as no model to assist the user in the grouping their friends no group based policy management approach has been implemented with privacy based on assistance scheme and clustering. No agreement between the users defined relationship clustering

1.4 Objective

Enabling the user privacy in the Social network has been implemented using Clustering techniques that assist users in grouping their friends for traditional group based policy management approaches. Identifying the example friends through associative policy templates and user policies user privacy, sentiment (i.e., an unconcerned user, a pragmatist or a fundamentalist), privacy management models can be automatically tailored specific to the privacy sentiment and needs of the user. Privacy management model - for memory management and opinion to set policy with respect to relation.

2. PROPOSED SYSTEM

The objective of the project is to preserve privacy through the following process and it will also reduce the human effects.

2.1 Privacy Improvement Techniques

- Clustering technique to group the friends
- Assisted Friend Grouping
- Same-As Policy Management
- Example Friend Selection

Human effects includes cluster/user defined relationship group alignment, user privacy sentiment, efficiencies and user perceptions

- **Designing the Assisted friend grouping**
  Here the solution enhances traditional group-based policy management approach. Assited Friend Grouping helps users in grouping their friends more effectively. It will club with clusters and user-defined relationship groups. It will increase more benifits in the social networks.
- **The assisted friend grouping is organised through clustering technique.**
  Function of clustering in grouping friend is to support users in maintaining the relationships between the groups. Here Clasuet Newman Moore (CNM) network clustering algorithm is used. This algorithm analyzes and detects community structure in networks by optimizing modularity. Modularity is a metric that describes the quality of a specific proposed division of a network into communities. Our prototype clusters the user's social network graph creating CNM clusters (or groups) of friends.
- **Assigning Permission**
  Permission is assigned through probability metrics policy and it also been utilized to guess the profile object data. In Group Based, users associate the policy with the group. while using Same-As, users associate the policy with a friend . this will help users in assigning the permissions and to be more selective.
- **Construction of Example friend Selection Method**
  Friend selection method is a pair wise comparison which has Bonferroni correction, where there is statistical significance. Author policies are done faster through CNM order because we have highly connected friends. The most highly connected friend of a cluster is presented first and it is selected as a Same-As Example Friend. this friend will be well known and therefore it is easier to remember to make good candidates. After the policy is being set, the stream of friends will be from same cluster and they will be showing same relationship group and policy template will be also same. The users mental model will be also based on Same-As Example Friend where they will be linked with same stream of friends.

2.2 Architecture

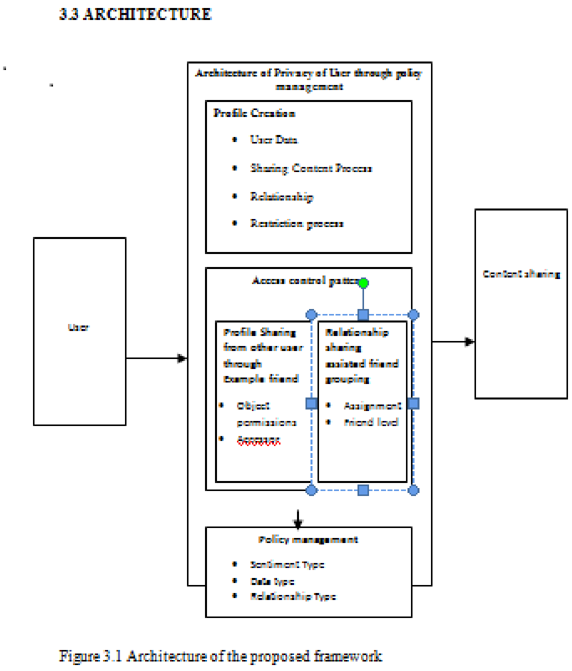

Figure 3.1 Architecture of the proposed framework

2.3 Advantages

- User Intended Friend selection for data sharing
- Effective memory management
- Privacy is preserved to a much extend through classification policies.

3. RELATED WORK

3.1 R. McMillan presented "Representing and reasoning about web access control policies".[25]

New technologies such as web services, service-oriented architecture, and cloud computing enables users to perform business services more effectively. But still problems like unintended security leakage by unauthorized services while using internet may occur to users. Lack of logical and formal foundation will cause errors in designing and managing web access policies. The web access control policy will be maintained by the Introduction of a logic based policy management approach and focused on XACML (extensible access control markup language, this is the basic standard for specifying and enforcing access control policies for various applications. Answer set programming (ASP) approach is adopted to formulate XACML to find the performance, logical reasoning and policy verification.

3.2 A. Acquisti and J. GrossklagsMoving beyond untagging: Photo privacy in a tagged world.[2]

Many social network sites that allows users to upload images add the feature of photo tagging with other users. Privacy of all these tagged images will be examined. Needs and concerns of the users will be explored and the privacy of the tagging will be considered. Now all the privacy mechanisms will be enhanced and it will be validated by mixing with other methods and implementing. As the privacy of photo tagging is that important the findings of using privacy tools will also be taken into consideration for better privacy management.

3.3 J. Bonneau and S. PreibuschAll your contacts are belong to us: automated identity theft attacks on social networks.[4]

Popularity of social networking sites have been increasing drastically. Facebook, well known social networking site shows a growth of 3% per week. Millions and millions of users are registering and using various social networking sites day by day, they share photographs contacts long lost friends, get business contacts and so on. Here we investigate how easily an attacker can attack a social network site and retrieve the data and other personal information about the users. As the initial step the attacker will send friend request to the user whose information is to be attacked and once request is accepted the attacker will retrieve the information of the user. Another case a forged profile will be created and the user will be asked to register in it and also contacts the friends of the user also to register and there by personal information of user could be retrieved.

4. EXPERIMENTAL ANALYSIS

4.1 Approach

Microsoft visual studio is used to implement user intended privacy preserving models in online social networks.

4.2 Implementation Phases

1. Building Utilities for an Online Social Network.
2. Designing a user-assisted friend grouping mechanism for managing the privacy.
3. Establishing Privacy Based on Privacy Paradox
4. Construction of Example Friend Selection Methods

4.2.1 Building a utilities for a Online Social Network

Building a Social network is to enable the user to share the information with respect to profile data, interest, activities and content. Profile data can be selfie images, Personal information's, Educational and Cultural information's. Social Network is to share and connect to other to data dissemination. Representation of the user is achieved by creating space to the load the data of the user and enables it to another user.

Utilities of the OSN

1. **Sharing the social links**
2. **Email**
3. **Instant Messaging**

Social network incorporate the new information, Photo and blogging. Online Community is established to allow users to share ideas, pictures, posts, activities, events, interests with people in their network. Some social networks have additional features, such as the ability to create groups that share common interests or affiliations, upload contents and hold discussions in forums.

4.2.2 Designing a user-assisted friend grouping mechanism for managing the privacy

Groups of users based on the relationship is enabled by user assisted friend grouping mechanism and object permissions will be given to the groups. In two areas assisted friend grouping extends,1)provides the user with assistance in grouping their friends, and 2)provides the user to do friend level exception with group policy. According to certain criteria's the privacy considerations will be done, social circles, tie strength, temporal episodes, geographical locations, functional roles, and organizational boundaries. In any friend grouping page each user is present at the center of the friend grouping page and the user is asked to select, for each friend the group that best friendship being represented. The friends can be either dragged by the users to the appropriate groups. Clasuet newman moore(CNM) network clustering algorithm is used to assist users in grouping their friends. By optimizing the modularity these clustering algorithm analyzes and detects community structure in networks. CNM group order will be considered while presenting friends to the users. once all friends are selected and grouped the user will set group policy by setting permissions that allow or deny access to users profile objects, e-mail address, photos and so on.

4.2.3 Establishing Privacy based on Privacy Paradox

Privacy paradox is established by the disclosure of the actual behavior of the user. Information disclosure is against the privacy strategies. Privacy paradox is maintained by privacy criteria's.

- **Designing the Assisted friend grouping**
  Assisted friend grouping leverages clustering algorithm to aid users in grouping their friends effectively and efficiently. Measurable agreements are done between clusters and user-defined relationship groups. More benefits to social networks through user perception improvements are caused.

The assisted friend grouping is organised through clustering technique.

Clustering algorithm in the friend grouping helps to assist users in populating their relationship groups, the Clasuet Newman Moore (CNM) network clustering algorithm is used as the clustering technique. Modularity could be found as the clustering algorithm analyzes and detects community structure in networks. The metric that describes the quality of a specific proposed division of a network into communities is modularity. Here it clusters the user's social network graph creating CNM clusters (or groups) of friends. The friends to the users will be presented in the CNM group order during friend grouping.

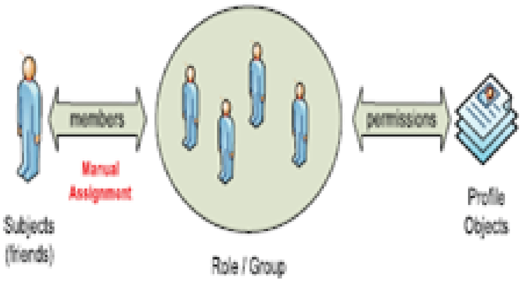

Figure4.2.3: Assisted friend grouping

- **Assigning Permission**
  Probability metrics provides permissions to groups. the policies will be assigned to a group by the users. In the same-as the policy will be associated with a friend and will be assigned. The users will be more selective and careful in assigning the permissions. The permissions will be given only to the most effective groups, this will improve the efficiency of the overall privacy concerns.

4.2.4 Construction of Example friend Selection Method

The friend selection example used in the proposed system is a comparison method which compares the pair of friends and observes the statistical significances of all available pairings. Authoring of policies are done with the help of a faster method which uses friends who are highly connected as same as example friends. First the system selects the highest connected friend of a cluster and recommended it as a same-as example friend. The selected most highly connected friend is the most popular one and he is easier to point out so that it can be easily selected in same-as example friends. So the system first the policies and then finds the group of friends from the same cluster and same relationship group and also from the same policy template. The system then associates the user mental model and also the group of friends within the same-as example friends. For each of the clusters of the users this process will repeat.

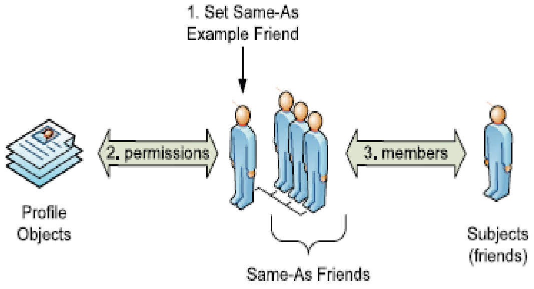

Figure4.2.4: Example friend selection

- **Policy Authoring Scheme**
  Policy Authoring Scheme is used to enable the private data access by checking the conditions of authoring such as the value of probability within the specific threshold value.

- **Privacy Sentiment**
  Flexibility problems arises because of the less expert users who may generate more open policies which will leads to coarse grained privacy management function. The system needs a fine grained approach in order to ensure better privacy which can be done with authoring more conservative policies. Privacy sentiments are enhanced for better management of user privacy information access in the privacy models.

5. CONCLUSION AND FUTURE WORK

New privacy management models have been introduced and thereby system has been implemented and designed and in addition their human effects were measured. Solution presents an enhancement to traditional group-based policy management, which assists users in grouping their friends more effectively. Solution introduces same as policy management, which leverages user’s opinion in example friend selection. Solution introduces two techniques in aiding users for selecting example friends. Privacy management models can be further enhancing by detecting and leveraging users privacy sentiment. For uncensored users, a more coarse-fine grained privacy management model could be leveraged and for fundamentalists, a more fine-grained approach could be used.

5.1 Future Work

Future work will be focusing on running and comparing two CNM -based policy management model enhancements which will include policy definition, openness, and their human effects. In addition it will further investigate patterns in alignment of clusters and user-defined relationship groups. System will also develop privacy sentiment for mass customization of privacy management.

6. ACKNOWLEEDGEMENT

First and foremost I place this project work on the feet of GOD ALMIGHTY who is the power of strength in each step of progress towards the successful completion of my project. I am highly indebted to Dr.N.R.Alamelu, M.E., Ph.D. Principal, Sri Ramakrishna Engineering College, Coimbatore for providing the required facilities and support to carry out this project work. I extend my heartfelt thanks to Dr.A.Grace Selvarani, M.E., Ph.D. Professor and Head, Department of Computer Science and Engineering (PG), who had been a source of inspiration and for her timely guidance in the conduct of this project work. I am grateful to Mr. Saravana kumar, assistant professor(senior grade), Department of Information Technology, for his able guidance and useful suggestions which helped me in completing the project work in time. Finally, I would like to express my heartfelt thanks to my beloved parents for their blessings, my friends for their help and wishes for the successful completion of this project.

7. REFERENCES

[1] Acquisti.A and Gross.R(2006), “Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook,” Proc. Sixth Int’l Conf. Privacy Enhancing Technologies (PET ’06.

[2] Acquisti.A and Grossklags.J(2005), “Privacy and Rationality in Individual Decision Making,” IEEE Security & Privacy, vol. 3, no. 1, pp. 26-33.

[3] Besmer.A, Watson.J(2010), and H.R. Lipford, “The Impact of Social Navigation on Privacy Policy Configuration,” Proc. Symp. Usable Privacy and Security,

[4] Bonneau.J and Preibusch.S(2009), “The Privacy Jungle: On the Market for Data Protection in Social Networks,” Proc. Workshop the Economics of Information Security (WEIS ’09).

[5] Carminative.B, Ferrari.E(2009), Heatherly.R, Kantarcioglu.M, and Thuraisingham.B, “A Semantic Web Based Framework for Social Network Access Control,” Proc. Symp. Access Control Models and TechnologieS.

[6] Carminati.B, Ferrari.E, Heatherly.R, Kantarcioglu.M, and Thuraisingham.B.M(2011), “Semantic Web-Based Social Network Access Control,” Computers & Security, vol. 30, pp. 108-115.

[7] Cheng.Y, Park.P, and Sandhu.R.S(2012), “A User-to-User Relationship- Based Access Control Model for

Online Social Networks," Proc. 26th Ann. IFIP WG 11.3 Conf. Data and Applications Security and Privacy.

[8] Clauset.A,Newman.M and Moore.C(2004), "Finding Community Structure in Very Large Networks," Physical Rev. E, vol. 70, p. 066111.

[9] Cutrell.E, Czerwinski.M, and Horvitz.E(2001), "Notification, Disruption, and Memory: Effects of Messaging Interruptions on Memory and Performance," Proc. Conf. Human Computer Interaction.

[10] Dhamija and Perrig.A(2000), "Deja Vu: A User Study Using Images for Authentication," Proc. USENIX Security Symp.

[11] Dunphy.P, Heiner.A.P, and Asokan.N(2010), "A Closer Look at Recognition-Based Graphical Passwords on Mobile Devices," Proc. Symp. Usable Privacy and Security.

[12] Dwyer.C, Hiltz.S.R, and Passerini.K(2007), "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace," Proc. Am. Conf. Information Systems (AMCIS '07).

[13] Fang.L and LeFevre.K(2010), "Privacy Wizards for Social Networking Sites," Proc. Conf. World Wide Web.

[14] Ferraiolo.D and Kuhn.R(1992), "Role-Based Access Control," Proc. Nat'l Computer Security Conf.

[15] Fong.P.W(2011), "Relationship-Based Access Control: Protection Model and Policy Language," Proc. Conf. Data and Application Security and Privacy.