Relationship Strength Based Privacy for the Online Social Networks

Javed Ahmed[1], Adnan Manzoor[2], Nazar H. Phulpoto[2], Imtiaz A. Halepoto[3], Muhammad Sulleman Memon[3]
[1]Department of Computer Science, IBA Sukkur University, Pakistan
[2]Department of Information Technology, QUEST Nawabshah, Pakistan
[3]Department of Computer Systems Engineering, QUEST Nawabshah, Pakistan

***Abstract*—The trend of communication is changing from mobile messages to the online social networks, for example, Facebook. The social networking applications and websites provide many of the characteristics, such as personal photo sharing. On the positive side by that many individuals form the social relationships. However, the online social networks may lead to the misuse of personal information and its disclosure. The social networks are static and assume equal values for the individuals who are directly connected. On the other hand, in real life the social relationships are dynamic and they are based on different attributes such as location, family background, neighborhood and many more. In order to be secure from the undesirable consequences due to personal information leakage, the effective mechanisms are required. In this paper, a model is proposed for the privacy in online social networks. The proposed model restricts the disclosure of personal information to the individuals. The information of one individual may be disclosed based on the relationship strength and the context. The implementation of this model on the social networks reduces the percentage of information disclosure to the less known individuals.**

***Keywords*—Online social networks; privacy; social relationships**

I. Introduction

Day by day increasing availability of the Internet also increase number of devices that are used for communication, such as mobile phones. These devices help in arranging the online streaming and conferencing. One of the main usages of these devices is the communication through the online social networks (OSNs). The users of phone spent unprecedented time while using the OSN websites. Many of the individuals also use OSNs for the business purpose to advertise the products. However, the in- formation sharing such as location sharing on the social networks may lead to information disclosure. Many of the user leave the privacy settings on of the social networks on default. As the meeting online is very different when compared with the meeting in real life. So, it is very important to protect your data and personal information. Due to which, the security and privacy concerns are getting attention of many networking communities [1]. With features available for the privacy settings, it is mentally fine to put the information on private. However, the social friendship with individuals may leak the information the attackers [2], Liu et al. [3]. Unlike social networks the relationships in real life evolve with time. So it also raises many questions regarding the maintenance of social relationships. In OSNs there is a need for a proper mechanism to manage social relationships of individuals in a dynamic environment with diverse audiences. The main motivation for this research is to develop a model to represent user's diverse social relationships on the basis of relational strength and social context. In everyday life relationship strength and social context are crucial factors to decide what to reveal and whom to reveal. Whereas, current OSNs offer friend as the only possible bidirectional relationship, which lack diversity in the type of social relationships which users form in everyday life. The objective of this research to design a model for social relationships in online social networks which mimic real life relationship forming pattern. More specifically, this paper provides the details of modeling dynamism, asymmetry, relational strength, and contextual integrity in user relationship in OSNs. The following questions are addressed:

- How to model user's relationship in online social networks?
- How to model user's relationship strength in online social networks?
- How to model user's contextual role in online social networks?
- How to model user's interactions in online social networks?

The study on audience segregation was conducted by Leenes et al. [4], where the authors develop an experimental online social network prototype known as the Clique. The Clique is inspired from Goffmans theory of self-presentation and offers the mechanism for audience segregation. The Clique required the users to invest energy and time to perform audience segregation. The study [5] based on the partitioning a users friends has also improved the privacy concerns. Authors in [6], [7] proposed the model for grouping social friends with matching characteristics in order to improve the privacy (see also [8]). The evaluation of privacy on social websites is also in consideration of many researchers [9]-[11].

II. Privacy: Theoretical Framework

One of the simplest definitions of privacy is the individual's claim and rights to control personal information from being access by the unauthorized or public. The information privacy on the social network is control by the individual and it is expected to remain safe from the disclosure [12]. Some of the well-know sources of online data such as:

- Location based applications
- Research and collaboration tools

- Online hospitals
- Online photo sharing
- Open access User profiles

One of the famous frameworks proposed for privacy of information is proposed in [13]. Where the focus was on the elements such as data integrity and privacy. The paper extends the idea over the social websites. Many of the researchers suggest that the information privacy and contextual integrity are related with each other [14], [15]. The authors in [16], [17] suggest the quality of relationship over the social networks plays a vital role in the minimization of information disclosure. In this paper, the proposed theoretical framework merges these social theories to address the multidimensional issue of privacy in social web. In following subsections, we illustrate the deficiency of existing privacy controls with help of problem scenarios that can be motivating factor to adapt our theoretical framework.

A. Contextual Integrity

Lets consider a simple example to understand the contextual integrity. Bob has several friends from his social life and he is also connected with his employer. Bob attain a social gathering near his city. Bob wishes to share the photos of party with his friends but not his office colleagues and employer. Currently all profile information of Bob is available to all his friends equally (by default). Among his friends, Bob also wishes to disclose photos to a limited number of friends depending on relationship context to avoid any embarrassing situation caused by revealing personal information to unintended audiences. One can argue that Bob can manage relationship context by creating lists and circles, whereas managing the appropriateness of these lists and circles is sole responsibility of the user. We know that social relationships are dynamic so maintaining the appropriateness of these static lists and circles is quite difficult and nearly impossible.

B. Disclosure Minimization

In reality social relationships are dynamic, and asymmetric in nature. Let us discuss a scenario to understand relationship dynamism. Alice started friendship with Bob almost five year ago. Alice has a new friend Eve on Facebook. With the passage of time Alice and Bob became the best friends. From the story is it observed that Alices relationship strength with Bob is strong, whereas relationship strength between Alice and Eve is weak. In future it is possible that Alice and Eve become the best friends. Moreover, it is also possible that the friendship between and Alice and Bob may break. Due to which, Alices relationship strength with Bob changes from strong to weak, and with Eve weak to strong. Consider another scenario to illustrate asymmetry in relationships. Bob is friend of his Boss on social networking site. Bob likes and comments positively on each post of his Boss. His Boss never commented or liked his status updates. It might be a mistake to consider Bob as close friend to his Boss. As interaction involve time and effort from participants. Bob has invested a lot of time, whereas, his Boss has invested no time. Boss has high influence on Bob, but Bob has no influence on his Boss. Influence is often asymmetric.

C. User Control

There are several occasions where the privacy of one individual be affected by the others, for example liking a post on Facebook. Photo Tagging is very common example of this phenomenon. The user controls are helpful in the situation. For example, on Facebook there is a control, which prevents others to tag you in a post or photo. The more advanced feature seeks permission from the tagged person before the use of tag. More examples of user controls are the setting of who can see the information you post.

III. Privacy Preserving Relationship Modeling

Our model addresses the issues of context collapse, maximum personal information disclosure, and lack of user control from sociological perspective. The proposed model is a modified version tie strength, contextual integrity, interpersonal boundary management and presentation of self. Such theories contains guidelines for individuals to control their personal information disclosure in face-to-face conservations. The domain of online social networks can also benefits from these foundational concepts of sociology. In following sections, we discuss building block of the model along with its formalism. The detailed description of social theories and their relationship with our model is avoided due to space limitations.

A. Preliminaries of the Model

OSNs are expressed by the number of users, relationship network, data collection and the user activity stream. Multiple criteria for classification of these OSNs entities is used. We benefit from research literature in privacy domain to identify these criteria [18]-[20]. Some of the factors used for classification are tie strength, information sensitivity, interaction intensity and user attitude towards privacy in online social networks.

1) Types of OSN Users: The users can be categorized depending on their behaviour and attitude towards privacy in online social networks. The attitude and the behavior are the key elements towards the information privacy. The privacy risks of each user can be determined by his usual behaviour and attitudes on OSNs. Following are the different types of OSN users [19]:

1. Socializers: The users join OSNs in order to make new friends just for the sake of entertainment. These users have large friend network but most of them are casual friends. The privacy policy suggested for these users is soft privacy.

2. Attention-Seeker: The users join OSNs to present themselves to the world. The users have extensive friend network, but they keep in active conversation with a limited number of friends. Generally, the privacy for these users is soft privacy.

3. Followers: The users join OSNs to keep up with what their peers are doing. The users have medium friend network. The privacy policy suggested for these users is hard privacy.

4. Faithful: The users join OSNs to rekindle old friendships. The users have medium friend network, most of their friends are from school or university. The privacy policy suggested for them is soft privacy.

5. Functionals: The users join OSNs for doing political campaigning, or charity work. The users have large friend network, most of their friends are of casual nature. The privacy policy suggested for them is hard privacy.

2) Types of social contexts: The relationship network of OSNs users is diverse in nature and users play several roles across different social contexts. Ozenc et al. [21] identified that three social contexts are very common among all OSNs users and needed management of intimacy levels within these social context for better social experience in online social networks.

1. Family: This context refers to relatives and can be inferred by analyzing profile attributes such as relationship status.

2. Work: This context refers to professional circle and can be inferred by analyzing profile attributes such as present and past work affiliations.

3. Social: This context refer to friends and can be inferred by analyzing profile attributes such as educational background, interests etc.

3) Types of social interactions: Online social networks provide rich set of user interaction for communication and information sharing and interaction pattern plays vital role to determine the quality of relationships among user in various social contexts.

1. Messaging: This refers to one to one communication method. Each message has sender, receiver, and content.

2. Posting: This refers to one to many communication method. Each post is created by certain user on specific user's wall with specific content, and certain set of audience.

3. Commenting: This is kind of post which is contribution in response to existing topic of discussion.

4. Tagging: This refers to sharing content with stakeholders.

5. Liking: This refers to contribution to existing post.

6. Chatting: This is kind of messaging which include session.

7. Wishing: This is kind of post that may include: creator, wall, data, and audience.

4) Grouping of user data: Since OSNs user share vast variety of multimedia content in their profile pages. Different data items may have different level of information sensitivity. Ho et al. [18] group user data into following categories depending on the sensitivity of information. This categorization can be useful in deciding privacy policy for OSN users.

1. Healthy: These users share data that is not harmful to anyone in terms of privacy.

2. Harmless: It is also like healthy data, which is used by marketing companies for business purpose.

3. Harmful: The disclosure of harmful data to inappropriate audience can create security and privacy risk.

4. Poisonous: The disclosure of poisonous data to audience other than strong ties can create security and privacy risk. This data contains information that can be help to track user or extract his financial information.

Ho et al. [18] also categorize shared data of OSNs users into five groups. All the data shared on OSNs falls into one of these groups. This grouping deals with nature of information contained in the data.

1. Identity: The data such as name or phone number, which is enough to identify a person.

2. Demographic: The data that contains the details such as gender, age, height, etc.

3. Relationships: The data refers to the relationship information of OSN users such as added friends, etc.

4. Activity: The data that shows the activities of a user.

5. Multimedia-content: The data refers multimedia, for example videos shared by the user.

Hu et al. [8] identified four different types of user privileges over data that can be important while assigning privacy policy:

i) Owner: The user is called owner of the data if it is contained in space of the user.

ii) Contributor: The user is called contributor of the data if it is commented or liked by the user.

iii) Stakeholder: The user is called stakeholder of the data if it tags the user.

iv) Disseminator: The user is called disseminator of the data if it is shared by the user.

5) Social relationship based privacy levels: The four privacy levels are suggested on the basis of relationships strength, social context and type of the users:

1. No-Privacy: This privacy policy is very liberal in nature. It allows everyone to access all type of user data.

2. Soft-Privacy: This privacy policy restricts access to poisonous data only to audience with strong ties, whereas healthy and harmless data is accessible to everyone. This policy is suitable for socializers, attention seekers, and faithfuls.

3. Hard-Privacy: This privacy policy allows everyone to access healthy data, whereas access to other types of data is restricted. This policy is suitable for followers and faithful users.

4. Full-Privacy: This privacy policy is very conservative in nature.

Table I represents various entities described in this section and highlights the their influence on each other. We describe privacy preserving social relationship model in next section using these building blocks.

B. Formalization of the Model

An OSN denoted by S is a 5-tuple and it is defined as: Users, Data, Relationships, Interactions, Policy. The description of each is given below.

TABLE I. PRIVACY POLICY FOR OSN USERS

Attributes	Socializer	Attention Seeker	Faithful	Follower	Functional
Friend Network	Large	Large	Small	Medium	Medium
Interaction Type	Photo Posting Photo Tagging Commenting Liking	Photo Posting Commenting Liking Wishing	Messege Chatting Wall Posting –	Commenting Liking Wall Posting –	Wall Posting Liking Commenting –
Relationship Strength	Weak Tie	Weak Tie	Strong Tie	Strong Tie	Weak Tie
Contextual Role	Social & Work	Social	Family & Social	Family & Social	Work & Social
Context Type	Harmful	Harmful Poisonous	Harmless	Harmless	Harmless
Privacy Policy	Soft Privacy	Soft Privacy	Hard Privacy	Hard Privacy	Soft Privacy

1) Users is the tuple: (U, Type, userType, Profile, userProfile, Policy, userPolicy, such as: U{u_1,$\cdots$,u_n} a finite set of OSN users identifiers. Type={Socializers, Attention-Seekers, Followers, Faithfuls, Functionals} userType= $U = 2^{Type}$ this is the case of assigns for each user at least one social category.

$Profile = \{p_1, , p_m\}$ is a finite set of profiles such that: $m \leq n$.

userProfile: $U - -2^{Profile}$ is a function that assigns for each user at least one profile.

Policy={No-Privacy, Soft-Privacy, Hard-Privacy, Full-privacy}

$userPolicy : Profile- > Policy$ is a function that assigns a privacy policy to each profile.

2) Data is the tuple: (D, Type, dataType, Sensitivity, dataSensitivit) $D = \{d_1, , d_m\}$ a finite set of data items represented by data identifier.

Type={Identity, Demographic, Relationship, Ativity, Multimedia-Content}

$dataType = D- > Type$ is a function that assigns for each data item a type.

Sensitivity={Healthy, Harmless, Harmful, Poisonous}

$dataSensitivity = D- > Sensitivity$ is a function that assigns sensitivity level to each data item.

3) Relationship is the tuple: (U,D,C,S,P,relU2U,relU2D,relD2D), where:

C={Social, Family, Work} is a set representing the relationship context.

S = attr_1: val_1,, attr_n:val_n this set represents relationship strength.

P = Owner, Stakeholder, Contributor, Disseminator represents users privilege over data items.

$relU2U = U \times U- > C \times S$ is a function to determine relationships among users.

$ErelU2D = UD- > 2^P$ is a function to determine relationship among user and data.

$relD2D = D- > 2^D$ is a function to determine relationship among different data resources.

4) Interactions is tuple (U, D, R, , Weight, History): = {Messaging,Posting,Commenting, Tagging,Liking,Chatting,Wishing} is set of actions

$Weight : - > [0, 1]$

$History : U- > 2$

5) Policy: It is an propositional logic formula over the set of parameterized actions.

An OSN is formalized using above mathematical representation that facilitates the system component description and manipulation. We describe formally all what is earlier mentioned in the previous section. The users are described as entities with type, profiles and their associated policies. In our formalism we represent all kind of relationship between the OSN entities and we annotate them with a weight value that characterize the strength of the relationship. The data items are considered as objects with the sensitivity dimension. We also take into consideration all kind of actions that are needed in the interactions between users themselves as well within the existing objects. Finally we describe a policy as a constraint taking the form of a propositional logic formula where the atomic propositions are the OSN entities values.

IV. CONCLUSION AND FUTURE WORK

With the growing number o smart phones as well as the Internet access. Moreover, the trend of using the social networking websites is also increasing. Due to the many social networking websites the data of users is available to the audience. This leads to the privacy concerns and disclosure of personal information. This paper presented a model based on the social relationships on OSNs. The model adopts the well know theories and decides the privacy concerns by defining weak and strong ties. The proposed model proved to minimize the disclosure of personal information. In future, the same work could be performed by using the ontological models for high performance.

REFERENCES

[1] Maritza Johnson, Serge Egelman, and Steven M Bellovin. Facebook and privacy: its complicated. In Proceedings of the eighth symposium on usable privacy and security, page 9. ACM, 2012.

[2] Cuneyt Gurcan Akcora and Elena Ferrari. Graphical user interfaces for privacy settings. In Encyclopedia of Social Network Analysis and Mining, pages 648660. Springer, 2014.

[3] Yabing Liu, Krishna P Gummadi, Balachander Krishnamurthy, and Alan Mislove. Analyzing facebook privacy settings: user expectations vs. reality. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, pages 6170. ACM, 2011.

[4] Ronald Leenes. Context is everything sociality and privacy in online social network sites. In Privacy and identity management for life, pages 4865. Springer, 2010.

[5] Fabeah Adu-Oppong, Casey K Gardiner, Apu Kapadia, and Patrick P Tsang. Social circles: Tackling privacy in social networks. In Symposium on Usable Privacy and Security (SOUPS), 2008.

[6] Anna Squicciarini, S Karumanchi, Dongyang Lin, and Nicole De-Sisto. Automatic social group organization and privacy management. In Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012 8th International Conference on, pages 8996. IEEE, 2012.

[7] Anna Squicciarini, Sushama Karumanchi, Dan Lin, and Nicole DeSisto. Identifying hidden social circles for advanced privacy configuration. Computers & Security, 41:4051, 2014.

[8] Hongxin Hu and Gail-Joon Ahn. Multiparty authorization framework for data sharing in online social networks. In Data and Applications Security and Privacy XXV, pages 2943. Springer, 2011.

[9] Eric Gilbert and Karrie Karahalios. Predicting tie strength with social media. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 211220. ACM, 2009.

[10] Eric Gilbert. Predicting tie strength in a new medium. In Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work, pages 10471056. ACM, 2012.

[11] Rongjing Xiang, Jennifer Neville, and Monica Rogati. Modeling relationship strength in online social networks. In Proceedings of the 19th international conference on World wide web, pages 981990. ACM, 2010.

[12] Jerry Kang. Information privacy in cyberspace transactions. Stanford Law Review, pages 11931294, 1998.

[13] Katrin Borcea-Pfitzmann, Andreas Pfitzmann, and Manuela Berg. Privacy 3.0:= data minimization+ user control+ contextual integrity. it-Information Technology Methoden und innovative Anwendungen der Informatik und Informationstechnik, 53(1):3440, 2011.

[14] Erving Goffman. The presentation of self in everyday life [1959]. Contemporary sociological theory, pages 4661, 2012.

[15] Helen Nissenbaum. Privacy as contextual integrity. Washington law review, 79(1), 2004.

[16] Irwin Altman. The environment and social behavior: Privacy, personal space, territory, and crowding. 1975.

[17] Mark S Granovetter. The strength of weak ties. American journal of sociology, pages 13601380, 1973.

[18] Ai Ho, Abdou Maiga, and Esma A13 053'fmeur. Privacy protection issues in social networking sites. In Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on, pages 271278. IEEE, 2009.

[19] Ofcom. Social networking: A quantitative and qualitative research report into attitudes, behaviours and use, 2008.

[20] Peter V Marsden and Karen E Campbell. Measuring tie strength. Social forces, 63(2):482501, 1984.

[21] Fatih Kursat Ozenc and Shelly D Farnham. Life modes in social media. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 561570. ACM, 2011.