Abstract— In the age of the Internet, privacy is a luxury and you have to constantly be on your heels to maintain it. OSN makes it particularly hard for users to guard their personal data. Besides many changes, Facebook privacy settings remain complicated. Even, past updates have unexpectedly made previously private information available to the public. It is difficult to balance the right of privacy and control of personal information when individuals voluntarily place personal information on their profile. Once information is placed on public domains users can easily lose control over who sees it and that may use it. While privacy settings are there to protect users, in practice this is not always the case, whether it is because of slack web design or through lack of knowledge or care by the user. Your data is shared more widely. Even if you have restricted your information to be seen by friends only, friends who are using a Facebook app could allow your data to be transferred to a third party without your permission. Remember: Sharing info with “friends of friends” could expose it to tens of thousands. A new approach is proposed to enable the protection of shared data in OSNs. A different Access control model is formulated to capture the essence of multiple authorizations, along with an access policy specification scheme and a policy mechanism. Along with, logical representation of access control model which allows us to leverage the features of existing logic solvers to perform various analysis tasks on our model. Here also discuss a proof-of-concept prototype as part of an application in Facebook and provide usability study and system evaluation of our method.

Keywords—privacy conflicts, online networks, security, protection, data sharing.

I. INTRODUCTION

Social networks such as Facebook, Twitter, and LinkedIn have an enormous volume of log data and user-generated content that researchers can mine to better understand user behavior both on- and offline [1, 2]. The exciting research challenge and opportunity for social network data is to paint a holistic view of users’ experiences and the boundaries of their interests and influence. Similar to Facebook in many facets, Renren (previously named Xiaonei, meaning “on campus”) is a large-scale, real-name (does not allow aliases) social network service (SNS) provider, designed as an interactive online environment for college students.

Registered users have personal homepages from which they can broadcast information and events, post blog entries, upload photos, make recommendations, and share others’ content. As with Facebook, these activities are broadcast to all the user’s friends. Although Renren has functionalities that are similar to Facebook, its interface and user population are different. Users can also communicate by commenting on one another’s guest books and uploaded content, or by posting short messages on their own pages. Figure 1 shows an example of a user’s personal homepage. The primary reason for the privacy issues in OSN is the centralized provider that stores and controls user data. Top social networking site are shown in Fig. 1.

Online social networking sites have become one of the greatest social technological phenomena of the 21st century [3]. However, most users are unaware of the many privacy issues that come with having a profile page on a social networking site. By placing personal information on the World Wide Web users make themselves vulnerable to online predators, selling of their information to third parties and in some instances, websites owning everything an individual places on their profile page or friend’s page, including photos. The problem is intensified because of the fact that communicating online via social networking sites has become not only popular but fashionable and for many young people, necessary to maintain their social status among friends. Because of this, young people are especially at risk of exposing themselves when sites are joined without any thought as to what may happen to personal information, photos and postings that are entered or placed on their or their friend’s profile pages. This paper looks at privacy issues of online social networking sites from around the world including Australia, USA, Japan, Korea, Brazil and India. It intends to raise awareness of privacy issues that people may face when creating their online identity with the hope that more care may be taken both by corporations and individual users.

When young people create personal profiles on line, they often include identifiable information like full names, date of birth, home town, school, relationship status, sexual preference, mobile numbers and email addresses.
PEW research on American teens showed that 82% of teens with online profiles post their first name, 79% a photo of themselves, 61% their city/town name, 49% include the name of their school and 29% their last name. Why young people are so willing to share personal information with often complete strangers they met online is an interesting phenomenon. A common misconception is that young people use social network sites to form new friendships or relationships, when in fact most use it to maintain connections that already exist.

Fig. 1: Top social networking sites

For example PEW research revealed that 90% of teens on MySpace use the service to stay in touch with people they already know. In Korea too, 85% of participants in a survey on Cyworld said they joined to maintain existing friendships. Given this, young people are more willing to place personal information on their profiles as they believe or assume that most people who will view their page will be ‘friends.’ However, it is much easier to become a ‘friend’ online than offline and many users do not restrict their privacy settings to only friends. The risk is illustrated by the PEW study which indicated that 31% of American teens with profiles have ‘friends’ who they have never met. These privacy concerns are further compounded by the new instant ‘chat’ feature where more personal conversations can take place with ‘friends.’

Personal information on social network sites is also being volunteered because of changing trends, increased familiarity and confidence in technology and lack of exposure or memory of misuse of personal data. It was also obvious from the survey that 18-34 year olds are much more likely to be comfortable providing detailed personal information to join social network sites than those above 50 years old. This is because young people have grown up with the internet where it has become normal to provide personal information to use certain online services.

According to ComScore up to end of November 2011,

<table>
<thead>
<tr>
<th>Table 1: Worldwide Unique Visitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook.com</td>
</tr>
<tr>
<td>Twitter.com</td>
</tr>
<tr>
<td>LinkedIn.com</td>
</tr>
<tr>
<td>Google+</td>
</tr>
<tr>
<td>MySpace</td>
</tr>
<tr>
<td>Others</td>
</tr>
</tbody>
</table>

II. Security Problems in Social Networks

One of the main concerns of social network providers is the security of user data. Users share personal data on social networks without being fully aware of consequences [3]. An individual’s context in the social network can be used to extract sensitive information. Using the context to extract information can be achieved through social phishing. For the security perspective, a social network can be treated as a graph and it is manipulated in some way to hide the information. The social networks providers need the private data for advertisement to generate revenues. Hence, it is a trade-off between providing security to users and releasing the same data to advertising companies. While the data are meant for the advertisers, attackers can take advantage of it as well. Providing this balance is challenging as the size and complexity of the data increases.
A. Anonymization

Social network providers use a variety of techniques to provide security. One popular algorithm is anonymization, which treats a social network as a graph and applies various transformations to it to achieve security [3]. Other algorithms include probabilistic modeling and decentralized modeling, which overcome the shortcomings of anonymization but have other issues such as complexity, trust and robustness. Although treating the social network as a graph has its own advantages, there are a few disadvantages too. The evolution of the graph over time can be modeled using link prediction algorithms and deanonymization algorithms can be used to extract information from the graph.

The strength of an algorithm can be measured in terms of information loss. Depending on what form of security the algorithm is providing, information and privacy loss measures can be used to compare different algorithms. The strength of an algorithm can be enhanced by recognizing and evaluating possible attack strategies. We can make algorithms robust against these attacks while maintaining its inherent strengths. Furthermore, we can work towards creating stronger algorithms which are not only secure computationally.

Facebook is a popular online social network. A user’s Facebook profile contains a wealth of personal information, including name, photo, and date of birth, contact information, relationship status, religious views, personal interests, hobbies, education history and more [4]. This information is made available to members of the user’s social network, allowing friends to stay in touch and up-to-date with each other’s lives. At the same time, Facebook generates revenue by targeting ads to highly specific demographics (e.g. single males between 18–24 years of age in New York City). Registering on Facebook under a pseudonym or obfuscating one’s personal information is forbidden by Facebook’s terms of service. Indeed, Facebook has banned users in cases where it identified violations of these terms. Although, negative publicity has forced Facebook to reinstate some user.

Based on the study conducted by Acquisti and Gross, Facebook users are concerned about who can access their personal information. While most users (60%) trust their friends almost completely with their personal information, significantly fewer (18%) trust Facebook (the company) to the same degree, and even fewer (6%) trust strangers. Yet, under the covers, Facebook allows any application developer (a stranger) access to a user’s profile [10]. While a privacy conscious user may choose to not use Facebook, finds that peer pressure drives membership.

III. HOW FACEBOOK EXPLOITS USER PRIVATE INFORMATION

You have willingly told Facebook who are your friends, what are your hobbies, how old you are, and your address and whether you are in a relationship or not. More, Facebook knows about what you like and dislike what your interests in, what your favorite movies and songs, simply from the updates you share and the ‘like’ buttons you press. The impotent question is: are you happy with Facebook to exploit about you?

The entire Facebook model is based on the effective use of your data. Here is the deal: they give you a free online social media platform to use and in turn sell advertising and based on what they learn about you. Today, Facebook has huge capabilities to collect, store and analyze data, what we call ‘big data analytic’. This allows Facebook to sell much targeted advertising - e.g. ‘someone living in the Mid-town district of Pune, who is single and who is interested in baseball and likes pizza’.

But Facebook goes beyond simply analyzing and ‘mining’ the user profile data you have shared and the updates you have written. In USA it is revealed how Facebook tracks you across the Web. Basically, when user creates an account, Facebook inserts a ‘tracking cookie’ into user Web browser that allows Facebook to track each website users are visiting. This means you are logged into Facebook and browse the web (completely separately from your Facebook activities) Facebook knows what different sites you are visiting.

There’s more: Cnet reports that whenever user click a Facebook 'like' button on any website, user preference is not only shared with user friends and on user profile, but data about user interests is sent back to Facebook’s servers, ready to sold to their advertising partners. More, personal data is exchanged when user use more apps with Friends via Facebook. It has been reported that signing up for these apps will give those companies who created the apps access to user personal data, even those details you specifically keep private on Facebook.

One more thing: Facebook has also invested in image processing and 'face recognition' capabilities, that basically allow Facebook to track user, because it knows what user and user friends look like from the photos user have shared. It can search the Internet and all other Facebook profiles that will find pictures of you and your friends. Face allows Facebook to make 'tag suggestions' for people on photos you have uploaded but it is overwhelming what else they could do with technology. Just guess how Facebook could use computer algorithms to track your body shape.
They could analyze your latest beach shots you have shared and compare them with older photo to detect that you have put on some weight. It could sell this information to a club in your area who can place an ad on your Facebook page.

Here are main questions: Are you comfortable with Facebook who is using your data? Or does this all feel a little too much like 'Big Boss is watching you'? Do you see it as a violation of your privacy and does you care about that Facebook knows everything about you and could exploit and sell? Does this make Facebook too much powerful? What do you think?

A. Control of Personal Information

Although in many ways a user offers 'consent' when they sign up to an online site, most are unaware of the implications of voluntarily providing personal information on profiles as well as not being aware of how this information may be processed [3]. An individual can lose control of their data when a digital dossier of personal information is generated. This occurs when profiles on social networks sites can be downloaded and stored over time by site operators for back up purposes so as incrementally create a digital dossier of personal information. This can also occur out of the control of the user as users’ ‘friends’ on their sites can write a comment about them on another friend's profile or ‘tag’ the individual in photos. It is in this way that profile in formation has the potential to be used in ways that the user did not intend and stored for n definite periods. Since the cost of disk storage and downloading is constantly being reduced, it is possible to take ‘snapshots’ of a whole network for storage or back up purposes. The main threat associated with digital dossier aggregation for young users is when future employees or colleges are able to perform searches that may bring up data or even compromising photos that an individual thought either no longer existed or not possible for that source to obtain. For example a gay student attending a Christian college in the US was expelled after administration officials viewed photos of the student dressed in drag on Facebook. Losing control in this way may be in conflict with the Purpose Specification and Use Limitation Principles as an individual’s personal data is not being used in a way they believed or told it would.

IV. DATA USE POLICY OF FACEBOOK

A. Information facebook receive

facebook receive a number of different types of information about you [21]:

Your information

Your information is the data that's required when user sign up for the site, as well as the information choose to share.

- Registration information

When user signs up for Facebook, user required to submit data such as your name, email address and birthday. In some cases, some other information need to be submit, like your telephone number, your current location.

- Information you choose to share

You can select information to share on Facebook, such as post a status update, upload a photo, or comment on a friend’s updates.

You can also include the information to share about your action, such as user add a friend, add a place to your story, like a Page or a website, or indicate you are in a relationship. User name, profile pictures, username and User ID are treated just like information you select to make public.

User birthday allows facebook to do things like show you age-appropriate content and advertisements.

B. Information others share about you:

Facebook receive information about user from user friends and others, such as when they upload user contact information, post a photo, tag user in a photo or status update, or add user to a group.
When people use Facebook, they may store and share information about other users, such as when they upload and manage their invites and contacts.

Other information Facebook receive about users. Facebook also receive other types of information about users:

- Facebook receive data about user whenever user interact with Facebook, such as when user look at another person's timeline, search for a friend or a Page, send or receive a message with others.
- When user post things like photos or videos on Facebook, Facebook may receive additional related data (or metadata), such as the time, date, and place user took the photo or video.
- Facebook receives data from the computer, mobile phone or other device user use to access Facebook, also when multiple users log up from the same device. This also includes your IP address and other information about things like user internet service, location, the type of browser user use. For example, Facebook may get user location information so Facebook can tell user if any of your friends are nearby.

Facebook also put together data from the information already have about you and your friends. For example, Facebook may put together data about which friends should show you in your News Feed or suggest you tag in the photos you post. They may put together your current city with GPS and other location information. For example, tell you and your friends about people nearby, or offer deals to you. They may also put together data about you to serve you ads that might be more relevant to you.

When get your GPS location, put it together with other location information they have about you (like your current city). But they only keep it until it is no longer useful to provide you services, like keeping your last GPS location to send you relevant notifications.

Facebook provide data to advertising partners or customers even after removed your name or any other personally identifying information from it.

C. Public information:

When you use the phrase "public information" which means that information selected to make it public and that is always publicly available.

D. Information you choose to make public:

Choosing to make your information public is exactly what it means: including people, anyone off of Facebook, will be able to see it.

Selecting to make your information public also means that this information:

- can be associated with you even off Facebook;
- can show up your information when someone does a search on Facebook or on a public search engine;
- It will be accessible to the Facebook, websites you and your friends use; and
- It will be accessible to anyone who uses our APIs such as our Graph API.

Sometimes you will not be able to select an audience when you post something for example when you write on a Page's wall or comment on a news article that uses comments plug-in. This is because some of stories are always public stories. In general, you should consider that if users do not see a sharing icon, that information will be publicly available.

When others share some information about you, they can select to make it public.

Always publicly available information is as follows:

- Name
  This helps your friends and family find you. Sometimes you are uncomfortable sharing your real name, they can always delete there account.
- Profile Pictures and Cover Photos
  These help your friends and family recognizes you. Sometimes users are uncomfortable making any of these photos public; you can always able delete it. Unless you delete them, will remain public in your profile picture or cover photo album.
- Network
  This helps you see whom you will be sharing information with before you choose "Friends and Networks" as a custom audience. If you don't want your network public, you may leave the network.
- Gender
  This allows us to refer to you properly.
International Journal of Emerging Technology and Advanced Engineering

• Username and User ID

These allow you to give a custom link to your timeline or Page, can able to receive email at your Facebook email address.

Usernames and User IDs

A Username (or Facebook URL) is a custom link to your timeline that you can give out to people or post on to external websites. Username visible in the URL on user’s timeline. Facebook also use your User ID to identify your account.

If someone wants to access your information and if they have your Username or User ID, they can access it through Facebook website. For example, if someone knows your Username, they can type URL like “facebook.com/Username” into their browser and see your public information. Similarly, someone with your Username or User ID can access information about you through APIs, such as Graph API.

If you do not want your information to be accessible or visible to Platform applications, from your privacy settings you can turn off all Platform applications. If you turn off Platform you will no longer be able to use any other applications until you turn on Platform. For more information that apps receive when you visit them, just see other websites and applications.

If you want to see information available about you through Graph API, just type “https://graph.facebook.com/” into browser.

V. RELATED WORK

Several proposals of an access control mechanisms for OSNs have been introduced (e.g., [6, 7, 8, 9, 10]). Carminati et al. [6] introduced a trust-based access control mechanism, which allows authorized users are denoted in terms of the depth, relationship type, and trust level between users in OSNs. They then presented a semi-decentralized discretionary access control system and an enforcement mechanism for controlled sharing of information in OSNs [7]. The D-FOAF system [20] is basically a friend of a friend ontology-based distributed identity management system, where relationships are associated with a level of trust, which represent the level of friendship between the users. Fong et al. [9] proposed an access control scheme that formalizes and generalizes the access control mechanism implemented in Facebook. Gates [11] described relationship-based access control as one of the new security paradigms that addresses basically the unique requirements of the Web 2.0.

Then, Fong [8] formulated this paradigm called a Relationship-Based Access Control (ReBAC). The ReBAC bases authorization decisions on the relationships between the resource owner and the resource accessor in an OSN. However, none of these presented works could analyze the privacy control requirements with respect to the collaborative data sharing in OSNs.

Several recent work [12, 13, 14, 15, 16] found the need of joint management for data sharing, especially photo sharing, in OSNs. Squicciarini et al. [15] provided a solution for collective privacy management for photo sharing in OSNs. This work recognized the privacy control of a content that is co-owned by multiple users, such that each co-owner may separately specify her/his own privacy control. The Clarke-Tax mechanism was adopted to enable the collective enforcement for shared content. Game theory was applied to evaluate the model. However, the main drawback of this solution is the usability issue, it could be very hard for ordinary OSN users to comprehend with the Clarke-Tax mechanism and specify proper bid values for auctions. Besides, the auction process adopted in the approach indicates only the winning bids could decide who was able to data access, instead of accommodating stakeholder’s privacy preferences. In Hongxin hu[19] proposes a simple but flexible mechanism for collaborative management of shared data in OSNs. In particular, they introduce an effective Conflicts resolution solution, which makes a tradeoff between privacy protection and data sharing considering the privacy concerns from multiple associated users.

Measuring privacy risk in OSNs has been proposed in several works [17, 18, 20]. Becker et al. [17] Presented PrivAware, a tool to detect and report unintended information loss through quantifying privacy risk associated with friend relationship. In [20], Talukder et al. proposed a privacy protection tool, called Privometer, which can measure the risk of potential privacy leak- age. Dayananth [18] presented a framework to compute the privacy score of a user, presenting the user’s potential risk caused by her/his participation in OSNs. The focused is also on the privacy settings of users with respect to their profile items. Compared with those existing work, this approach measures the privacy risk caused by different privacy concerns from multiple users, covering profile sharing, friendship sharing and content sharing. It also analyzes tasks on access control model used in OSNs.
VI. PROPOSED WORK

In Proposed System implemented a proof-of-concept for Facebook application for the Photo sharing in application server, called FBController. FBController is developed as third-party application in J2EE which is hosted in an Apache Tomcat application server supporting web technologies such as Html, JavaScript, CSS and database MySQL. FBController can access user’s basic information and content. It can retrieve and list all photos which are uploaded by the user and where the user was tagged. Then user can access FBController through its application page on Facebook where user can access information and set its privacy limitations. This approach follows relationship based access model to specify attribute relation with all other users connected with through Facebook. Privacy conflict occurs when two users disagree on whom the shared data item should be exposed to. Hence the important to consider tradeoff between privacy protection and data sharing when resolving privacy conflicts.

The main goal is:

d) To provide Security policies.

d) To handle Unauthorized Excess Control.

c) Provide policy and privacy for multiple users to specify there authorization.

d) Discover multiple activities using collaborative control.

e) An Online Social Network with User Control Privacy.

VII. CONCLUSION

The photo sharing through online social networking are allowing huge amount of people to upload and socially communicate. Such as, users have lost control over their identity and disclosures as other users can upload and tag undesired photos. More additionally, users are struggling to manage their identity through the contents of photos across multiple audiences and the many people in their social networks. Users need some more tools to allow them to regain control over their privacy of profile, and manage their privacy decisions. Users want these tools to respect everyone’s rights and provide a fair playing ground. As in being driven by impression management concerns, users also not motivated to change their behavior or use tools that do not fit in with their existing activities or that protect against other potential threats such as strangers using photos to infer personal information or location.

Facebook already have extensive privacy control, users did express desire for more fine-grained controls over the accessibility of individual photos linked with. While this study focused on Facebook adding similar features in other social networking sites. For example, MySpace recently added the ability to tag photos. Thus, the concerns and issues discovered will be applicable to other social networking sites with photo sharing. All these sites continue to grow in popularity and users add more and more photos, the user privacy needs is important to allow safe and comfortable participation on these online communities.

REFERENCES


