AUTOMATIC PRIVACY PROTECTIVE AGREEMENT FOR ONLINE SOCIAL NETWORK (OSN)

[1] **Dr S. KISHORE VERMA,** [2] **A. SANDEEP,** [3] **M. SHARADHA**

[1]Associate Professor, Department of Computer Science and Engineering,

[2, 3] Assistant Professor, Department of Computer Science and Engineering, Sri Indu College of Engineering and Technology, Hyderabad, Telangana-501510

ABSTRACT

In online social networks (OSNs), users are allowed to create and share content about themselves and others. When multiple entities start distributing content, information can reach unintended individuals and inference can reveal more information about the user. Existing applications do not focus on detecting privacy violations before they occur in the system. This project proposes an agent-based representation of a social network, where the agents manage users' privacy requirements and create privacy agreements with agents. An agent checking for current state to monitor. Agent not only protects privacy information of OSN user and also monitoring if any emergency or important information is protected with user privacy restriction. If there is any information on user account with privacy restriction, agent will resolve this by changing privacy information to public for reaching that information to more people.

Index Terms*—Privacy, Social networks, Privacy setting, Agent monitor.*

INTRODUCTION

The violations of privacy on social networks resembles violations of controlling access such as access control scenarios, single authority of granting accesses. However, in social networks, there are multiple sources of control. That is, each user can contribute to the sharing of content by putting up posts about as well as others. Further, audience of a post cans retrieve the content, making it accessible for others [1]. These interactions lead to privacy violations, some of which are difficult to detect by users. Review of is the main contributor to situation. This could be the user putting up a content that reveals unwanted information or it could be other people sharing content that reveals information about the user. The second axis is how the data is revealed; if the data was itself unwanted or the data led to new information being revealed (i.e., through inferences). According to these two axes, we identified four types of privacy violations. A user shares some content with some privacy settings, the system acts against these settings and shares the content with people that it was not supposed to. The information about a user is shared by another person. In online social networks, information about a user can easily propagate in the system, without a user's consent [2].

User puts up content on the social network without realizing that more information can be inferred from her post; e.g., giving away location information through a landmark. The friend's action leads to a privacy leakage but the leakage can only be understood with some inferences in place; e.g., a friend's tag revealing friendship status. Moreover, content may lead to privacy violations because of its semantics. A post may annoy or insult the user, or it may include private information; e.g., sharing a post that reveals the user's politic affiliation [3].

In this paper we have developed an approach for managing users' privacy constraints in social networks by detecting the violations of privacy and guide them. The project proposes an agent-based representation of a social network, where the agents manage users' privacy requirements and create privacy agreements with agents. An agent checks the current state of the system to resolve privacy violations before they occur. Agent not only protects from privacy information of OSN user and also monitoring if any emergency or important information is protected with user privacy restriction. The agent will resolve privacy information into public for reaching that information to more people [4].

RELATED WORKS

Friend recommendation is an important recommender application in social Media. Major social websites such as Tweet and Facebook are all capable of recommending friends to individuals. However, most of these websites use simple friend recommendation algorithms such as similarity, popularity, or "friend's friends are friends", which do not satisfy the majority of users [5]. They have developed an algorithm for Network Correlation-based Social Friend Recommendation. To accomplish this goal, we correlate different "social role" networks, find their relationships and make friend recommendation.. After important feature selection we recommend friends based on these features. They conducted experiments on the Flickr network, which contains more than ten thousand nodes and over 30 thousand tags covering half million photos, to show that the proposed algorithm recommends friends more precisely than reference methods [6].

For each social role, he/she makes different friends, and these different social roles form different social networks. To consider the effect of different social roles, they propose a network alignment method to find the correlations among different networks. The second aspect we take into account is the pairwise user similarity preservation to maintain the original data structure [7]. Experimental results have shown that the proposed NC-based SFR outperforms other methods in friend recommendation by aligning tag and contacts networks. They achieved the highest precision in friend prediction. They founded that a small number of features can align the tag network to contact network well and provide sufficient information for friend recommendation.

As social network expands, a user's privacy protection goes beyond his privacy settings and becomes a social networking problem. In this research, they aimed to address some critical issues related to privacy protection: Would the highest privacy settings guarantee a secure protection? Given the open nature of a social networking site, is it possible to manage one's privacy protection? With the diversity of one's social media friends, how can one figure out an effective approach to balance between vulnerability and privacy? They presented a new way to define a vulnerable friend from a private user's perspective which depend on whether or not the user's friends' privacy settings protect the friend and the individual's network of friends [8].

This work provides a large-scale evaluation of new security and privacy indexes using a Facebook dataset. They present and discuss a new perspective for reasoning about so- cial networking security. When a user accepts a new friend, the user should ensure that the new friend is not an increased security risk with the potential of negatively impacting the entire friend network [9]. Additionally, by leveraging the indexes proposed and employing new strategies for unfriending vulnerable friends, it is possible to further improve security and privacy without changing the social networking site's existing architecture.

They found that users are either not careful or not aware of security and privacy concerns of their friends. Their model clearly highlights the impact of each new friend on a user's privacy. There are vulnerable friends on social networking sites and it is important to find vulnerable friends so that users can improve their privacy and security. Removing vulnerable friends from a user's social network might decrease the utility of the social networking service from a social perspective but this strategy improves security and helps defend privacy. They are also interested in investigating the role of user vulnerability across social networks and relationship between the inertial user and vulnerable user [10].

As an outcome of the above problems, there are many malicious apps on Facebook every day. Because user has very incomplete material at the time of installing an app on his Facebook profile as user does not identify the proposed app is malicious or not only the identity number (the unique identifier assigned to the app by Facebook) Currently, there is no commercial service or research-based tool for advising a user about the risks of an app. Malicious apps are easily being spread, and because of it safety is compromised. There have been several researches done regarding spam and malware on Facebook which have focused on detecting malicious posts and social spam campaigns [11]. A recent study has shown how app authorizations correlate to privacy risks of Facebook apps. Finally, there are some community-based feedback driven efforts to rank applications, such as What app; though these could be very controlling in the future, so far they have received little acceptance [12].

System detected generally 200,000 malicious wall posts with embedded URLs, originating from more than 57,000 user accounts. Authors found that extra than 70% of all malicious wall posts advertise phishing sites. To study the distinctiveness of malicious accounts, and see that more than 97% are compromised accounts, rather than “fake” accounts formed solely for the principle of spamming. Finally, when adjusted to the local time of the sender, spamming dominates actual wall post in the early morning hours when users are normally asleep [13].

Application present a convenient means for hackers to spread malicious content on Facebook. User on facebook can only get request from benign apps. It provides security to users profiles from malicious apps. An application presents a convenient means for hackers to spread malicious content on Facebook. However, little is understood about the characteristics of malicious application and how they operate. In this , using a large corpus of malicious Facebook apps observed over a nine month period and showed that malicious apps differ significantly from benign apps with respect to several features. Leveraging our observations, developed FRAppE, an accurate classifier for detecting malicious Facebook applications [14].

As we all know, On-line Social Networks (OSNs) are very popular medium to communicate, share and a considerable amount of human life information. Daily and continuous communications, But it is very important for On-line social networks, to avoid unwanted messages getting displayed onto user walls. But OSNs provide very little support to this requirement [15]. To achieve this requirement, They proposed a system letting OSN users to have a direct control on the messages posted on their walls. They did this through a flexible rule-based system, which allows users to adapt the filtering criteria to be applied to their walls, and a Machine Learning classifier technique which automatically generates membership labels in support of content-based filtering [16].

But no support for content based preferences. Traditional classification techniques are not suitable for short text messages, as these short messages do not provide sufficient word occurrences. Therefore here our purpose is to offer a system, which automatically filters unwanted messages from OSN user walls This is a flexible rule-based system, which allows users to adapt the filtering criteria to be applied to their walls, and a Machine Learning classifier technique which automatically generates membership labels in support of content-based filtering. They used Machine Learning (ML) text categorization techniques to allot each short text message to its respective category [17].

They have presented an unwanted text message filtering from OSN user walls. The system uses a ML soft classifier to enforce customizable content-based FRs. Furthermore, the flexibility of the system in terms of filtering options is boosted through the management of BLs. The use of machine learning text classification technique makes classification more automatic and more efficient. The present batch learning strategy, based on the preliminary collection of the entire set of labeled data from experts, permitted an accurate experimental evaluation but needs to be developed to include new operational requirements. Our plan is to solve this problem by investigating the use of online learning paradigms able to include label feedbacks from users in future work. The proposed system may have problems similar to those encountered in the specification of OSN privacy settings [18].

PROPOSED APPROACH

Preserving privacy has long been an important mission of Web systems. The general process of preserving privacy is through privacy agreements. Web systems announce their policies through privacy agreements. To avoid this problem in this work we propose agent-based representation for detect privacy violation and to share important information to multiple user. The agent-based representations of social networks based on agents manage users' privacy requirements and create privacy agreements with agents. An agent monitoring the uploaded post, if the post is emergency automatically agent will change privacy information into public information

SOCIAL NETWORK DATASET

In this process, initially username and password details of users in social network such as Facebook datasets are collected. To enter the social network the users have to enter username and password. Users enter the valid username and password in a system to login successfully.

PRIVACY SETTING

While the user uploading the data or post he/ she have to set the privacy like public, friends and friends only. After setting the privacy the user can upload the post securely. If he set the privacy as public the mutual friends can see and share the user uploaded post. The public user can view only not able to share.

AGENT MONITOR

The agent will monitor a uploaded information based on post and check the post type. The agents manage users' privacy requirements and create privacy agreements. An agent checks the current state of the system to resolve privacy violations before they occur. Agent not only protects privacy information of user and also monitoring the user upload posts.

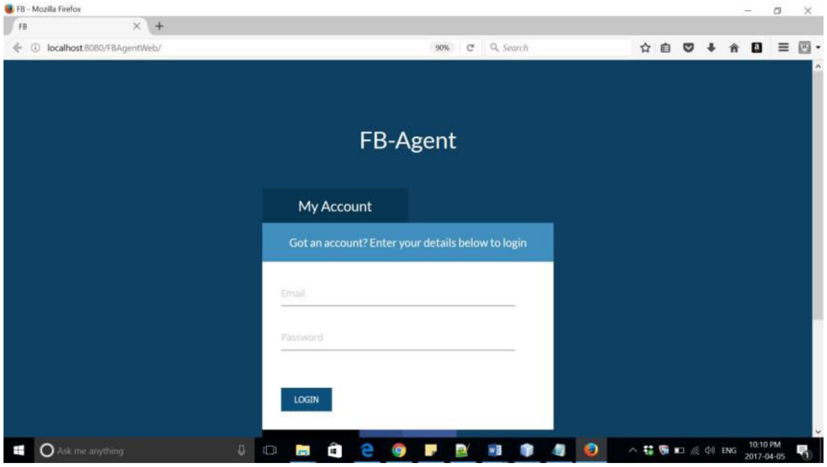
AGENT PERMISSION

The agent protected with user privacy restriction. The agent validates uploaded user post based on any emergency or important information, the agent will resolve by changing privacy information to public for reaching that information to more people. The uploaded post based on privacy information, the agent will resolve by changing public to privacy information.

EXPERIMENTAL APPROACH

Monitoring the privacy setting in such a way that the privay can be handled by the agent.After logging into the Facebook a user can post or share something like emergency information or private information on their fb account. Sometime we may forget to change our privacy setting and it may lead to inconvenience for that an agent is introduced here to frequently change the privacy setting.

Run the FB Client.java



FB - Mozilla Firefox

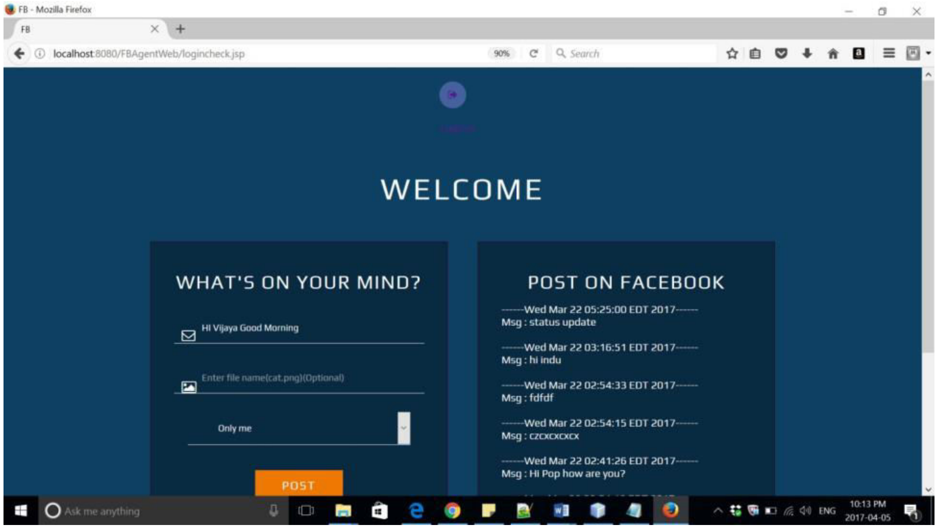
localhost:8080/FBAgentWeb/

FB-Agent

My Account

Got an account? Enter your details below to login

Posting some information.



FB - Mozilla Firefox

localhost:8080/FBAgentWeb/logincheck.jsp

WELCOME

WHAT'S ON YOUR MIND?

HI Vijaya Good Morning

Enter file name(cat.png)(Optional)

Only me

POST

POST ON FACEBOOK

-------Wed Mar 22 05:25:00 EDT 2017-------
Msg : status update

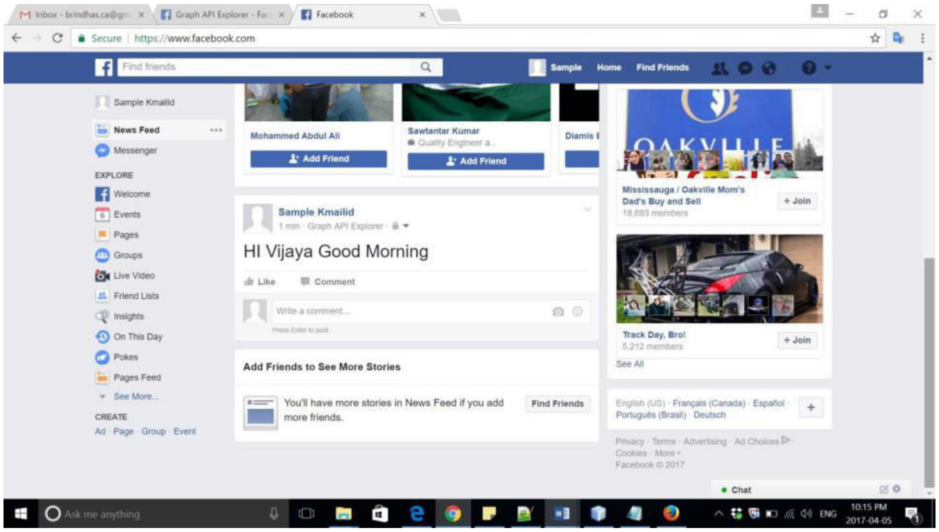
-------Wed Mar 22 03:16:51 EDT 2017-------
Msg : hi indu

-------Wed Mar 22 02:54:33 EDT 2017-------
Msg : fdfdf

-------Wed Mar 22 02:54:15 EDT 2017-------
Msg : czcxcxcxcx

-------Wed Mar 22 02:41:26 EDT 2017-------
Msg : Hi Pop how are you?

Then the agent will change after posting according to it.



https://www.facebook.com

Sample Kmailid
1 min · Graph API Explorer

HI Vijaya Good Morning

Add Friends to See More Stories

You'll have more stories in News Feed if you add more friends.

CONCLUSION

As social network usage is increasing day by day, privacy concerns are becoming more and more important. Social network users generally have multiple social network accounts for different purposes and in each network they will be sharing their personal information. This introduced a meta-model to define online social networks as agent-based social networks to formalize privacy requirements of users and their violations. In order to understand privacy violations that happen in real online social networks, we have conducted a survey with Facebook users and categorized the violations in terms of their causation. An agent checks the current state of the system to resolve privacy violations before they occur. Moreover, agents may have conflicting privacy requirements.

REFERENCES

[1] N. Kokciyan and P. Yolum. Commitment-based privacy management in online social networks. In First International Workshop on Multiagent Foundations of Social Computing at AAMAS, 2014. Facebook web site. http://www.facebook.com. Accessed: 2014-11-11.

[2] B. K. Samanthula and W. Jiang. An efficient and probabilistic secure bit-decomposition and its application to range queries over encrypted data. In Proceedings of the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS), pages 541–546. ACM, 2013.

[3] L. Andrews. I know who you are and I saw what you did: Social networks and the death of privacy. Simon and Schuster, 2012.

[4] R. Aydogan and P. Yolum. Learning opponent's preferences for effective negotiation: an approach based on concept learning. Autonomous Agents and Multi-Agent Systems, 24(1):104–140, 2012.

[5] B. K. Samanthula and W. Jiang. Structural and message based private friend recommendation. In Proceedings of IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pages 684–690. IEEE Computer Society, 2012.

[6] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove. An analysis of social network-based sybil defenses. In Proceedings of the ACM SIGCOMMconference, pages 363–374. ACM, 2010.

[7] X. Xie. Potential friend recommendation in online social network. In IEEE/ACM International Conference on Cyber, Physical and Social Computing and International Conference on Green Computing and Communications, pages 831–835. IEEE Computer Society, 2010.

[8] J. Sun, X. Zhu, and Y. Fang. A privacy-preserving scheme for online social networks with efficient revocation. In Proceedings of the 29th conference on Information communications (INFOCOM), pages 2516–2524. IEEE, 2010.

[9] K. Bhargavi. An Effective Study on Data Science Approach to Cybercrime Underground Economy Data. Journal of Engineering, Computing and Architecture.2020;p.148.

[10] M. Kiran Kumar , S. Jessica Saritha. AN EFFICIENT APPROACH TO QUERY REFORMULATION IN WEB SEARCH, International Journal of Research in Engineering and Technology. 2015;p.172

[11] K BALAKRISHNA,M NAGA SESHUDU,A SANDEEP. Providing Privacy for Numeric Range SQL Queries Using Two-Cloud Architecture. International Journal of Scientific Research and Review. 2018;p.39

[12] K BALA KRISHNA, M NAGASESHUDU. An Effective Way of Processing Big Data by Using Hierarchically Distributed Data Matrix. International Journal of Research.2019;p.1628

[13] P.Padma, Vadapalli Gopi,. Detection of Cyber anomaly Using Fuzzy Neural networks. Journal of Engineering Sciences.2020;p.48.

[14] Kiran Kumar, M., Kranthi Kumar, S., Kalpana, E., Srikanth, D., & Saikumar, K. (2022). A Novel Implementation of Linux Based Android Platform for Client and Server. In A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems (pp. 151-170). Springer, Cham.

[15] Kumar, M. Kiran, and Pankaj Kawad Kar. "A Study on Privacy Preserving in Big Data Mining Using Fuzzy Logic Approach." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 11.3 (2020): 2108-2116.

[16] M. Kiran Kumar and Dr. Pankaj Kawad Kar. "Implementation of Novel Association Rule Hiding Algorithm Using FLA with Privacy Preserving in Big Data Mining". Design Engineering (2023): 15852-15862

[17] K. APARNA, G. MURALI. ANNOTATING SEARCH RESULTS FROM WEB DATABASE USING IN-TEXT PREFIX/SUFFIX ANNOTATOR, International Journal of Research in Engineering and Technology. 2015;p.16.

[18] Y. Ding, Y. Hu, K. Hao, and L. Chen, ``MPSICA: An intelligent routing recovery scheme for heterogeneous wireless sensor networks,'' Inf. Sci., vol. 308, pp. 49-60, Jul. 2015.