ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Privacy Protection Online Social Media

[1] Dr.A.Ramamurthy, [2] P.Jyothi, [3] K.Swathi
[1] Professor, [2] [3] Asst. Professor
[1][2][3] Department of CSE, Teegala Krishna Reddy Engineering College

Abstract:- **Items shared through Social Media may affect more than one user's privacy e.g., photos that depict multiple users, comments that mention multiple users, events in which multiple users are invited, etc. The lack of multi-party privacy management support in current mainstream Social Media infrastructures makes users unable to appropriately control to whom these items are actually shared or not. Computational mechanisms that are able to merge the privacy preferences of multiple users into a single policy for an item can help solve this problem.However, merging multiple users' privacy preferences is not an easy task, because privacy preferences may conflict, so methods to resolve conflicts are needed. Moreover, these methods need to consider how users' would actually reach an agreement about a solution to the conflict in order to propose solutions that can be acceptable by all of the users affected by the item to be shared. Current approaches are either too demanding or only consider fixed ways of aggregating privacy preferences. In this paper, we propose the first computational mechanism to resolve conflicts for multi-party privacy management in Social Media that is able to adapt to different situations by modeling the concessions that users make to reach a solution to the conflicts. We also present results of a user study in which our proposed mechanism outperformed other existing approaches in terms of how many times each approach matched users' behaviour.**

I. INTRODUCTION

Data Mining is an analytic process designed to explore data (usually large amounts of data - typically business or market related) in search of consistent patterns and/or systematic relationships between variables, and then to validate the findings by applying the detected patterns to new subsets of data. The ultimate goal of data mining is prediction - and predictive data mining is the most common type of data mining and one that has the most direct business applications. The process of data mining consists of three stages: (1) the initial exploration, (2) model building or pattern identification with validation/verification, and (3) deployment (i.e., the application of the model to new data in order to generate predictions). Stage 1: Exploration: This stage usually starts with data preparation which may involve cleaning data, data transformations, selecting subsets of records and - in case of data sets with large numbers of variables ("fields") - performing some preliminary feature selection operations to bring the number of variables to a manageable range (depending on the statistical methods which are being considered). Then, depending on the nature of the analytic problem, this first stage of the process of data mining may involve anywhere between a simple choice of straightforward predictors for a regression model, to elaborate exploratory analyses using a wide variety of graphical and statistical methods (see Exploratory Data Analysis (EDA)) in order to identify the most relevant variables and determine the complexity and/or the general nature of models that can be taken into account in the next stage. Stage 2: Model building and validation: This stage involves considering various models and choosing the best one based on their predictive performance (i.e., explaining the variability in question and producing stable results across samples). This may sound like a simple operation, but in fact, it sometimes involves a veryelaborate process. Stage 3: Deployment. That final stage involves using the model selected as best in the previous stage and applying it to new data in order to generate predictions or estimates of the expected outcome. The concept of Data Mining is becoming increasingly popular as a business information management tool where it is expected to reveal knowledge structures that can guide decisions in conditions of limited certainty. Recently, there has been increased interest in developing new analytic techniques specifically designed to address the issues relevant to business Data Mining (e.g., Classification Trees), but Data Mining is still based on the conceptual principles of statistics including the traditional Exploratory Data Analysis (EDA) and modeling and it shares with them both some components of its general approaches and specific techniques.

II. RELATED WORKS

Resolving multi party privacy conflicts in social media [2016]

Items shared through Social Media may affect more than one user's privacy e.g., photos that depict multiple users, comments that mention multiple users, events in which multiple users are invited, etc. The lack of multi-party privacy management support in current mainstream Social Media infrastructures makes users unable to appropriately control to whom these items are actually shared or not. Computational mechanisms that are able to merge the privacy preferences of multiple users into a single policy for an item can help solve this problem. However, merging multiple users' privacy preferences is not an easy task, because privacy preferences may conflict, so methods to resolve conflicts are needed. Moreover, these methods need to consider how users' would actually reach an agreement about a solution to the conflict in order to propose solutions that can be acceptable by all of the users affected by the item to be shared. Current approaches are either too demanding or only consider fixed ways of aggregating privacy preferences. In this paper, we propose the first computational mechanism to resolve conflicts for multi-party privacy management in Social Media that is able to adapt to different situations by modeling the concessions that users make to reach a solution to the conflicts.

Estimating age privacy leakage in online social network [2012]

We perform a large-scale study to quantify just how severe the privacy leakage problem is in Facebook. As a case study, we focus on estimating birth year, which is a fundamental human attribute and, for many people, a private one. Specifically, we attempt to estimate the birth year of over 1 million Facebook users in New York City. We examine the accuracy of estimation procedures for several classes of users: (i) highly private users, who do not make their friend lists public; (ii) users who hide their birth years but make their friend lists public. To estimate Facebook users' ages, we exploit the underlying social network structure to design an iterative algorithm, which derives age estimates based on friends' ages, friends of friends' ages, and so on.We find that for most users, including highly private users who hide their friend lists, it is possible to estimate ages with an error of only a few years. We also make a specific suggestion to Facebook which, if implemented, would greatly reduce privacy leakages in its service

Measuring privacy risk in social network [2009]

In Facebook, when Bob visits Alice's profile page, the information that is displayed to him depends on his relationship with Alice (for example, whether she is a friend or not) and on Alice's privacy settings. Roughly speaking, when Alice is a Facebook friend of Bob, then he typically gets to see Alice's full profile page, which includes links to all of Alice's friends as well as all of the information and photos that Alice puts into Facebook; if Alice is not a friend, Bob only gets to see a limited profile page, which often includes no more than Alice's full name and her photo. we focus on estimating birth year, which is a fundamental human attribute and, for many people, a private one. We have found that in this sample dataset of 1.47 million usersfrom New York City, only 1.5% of them specify their age in theirpublic profile, confirming that age is indeed a private attribute for most users. Motivated by this, we ask the question: with what level of accuracy is it possible to estimate the age of the remaining users – i.e., those who aim to hide their ages – witha high accuracy? We seek to answer this question using algorithms that are note Facebook specific, so that they can be applied to OSNs in general. For age estimation, we only use public profile and friendship information; we do not use image analysis or network/group information.

III. METHODOLOGY

Children's advocacy groups and modern society at large recognize the importance of protecting the Internet privacy of minors (less than 18 years of age). Online Social Networks, in particular, take precautions to prevent third parties from using their services to discover and profile minors. These precautions include banning young children from joining, not listing minors when searching for users by high school or city, and displaying only minimal information in registered minors' public profiles, no matter how they configure their privacy settings.

Traditional Web-based educational systems still have several shortcomings when comparing with a real-life classroom teaching, such as lack of contextual and adaptive support, lack of flexible support of the presentation and feedback, lack of the collaborative support between students and systems. Based on the educational theory, personalization increases learning motivation, which can increase the learning effectiveness. A Fuzzy K-Logic method has been built to present student's knowledge state, while the course content is modeled by the concept of context. By applying such Fuzzy K-Logic logic, the content model, the student model, and the learning plan have been defined formally. A multi-agent based student profiling system has been presented. Our profiling system stores the learning activities and interaction history of each individual student into the student profile database. Such profiling data will be abstracted into a student model. Based on the student model and the content model, dynamic learning plans for individual students will be made. Students will get personalized learning materials, personalized quiz, and personalized advices. In order to understand the students' perception of our prototype system and to evaluate the students' learning effectiveness, a field survey has been conducted. The results from the survey indicate that our prototype system makes great improvement on personalization of learning and achieves learning effectiveness than FB would normally reveal for a child, including information about other minor friends who hadn't misstated their ages.

IV. SYSTEM ANALYSIS AND DESIGN

Existing system

In existing work with modest crawling and computational resources, and employing data mining heuristics, can circumvent these precautions and create extensive profiles of tens of thousands of minors in a targeted geographical area. In particular, using Online Social Networks and for a given target high school, we construct an attack that finds most of the students in the school, and for each discovered student infers a profile that includes significantly more information than is available in a registered minor's public profile. An attacker could use such profiles for many nefarious purposes, including selling the profiles to data brokers, large-scale automated spear-phishing attacks on minors, as well as physical safety attacks such as stalking, kidnapping and arranging meetings for sexual abuse. Ironically, the Children's Online Privacy Protection Act (COPPA), a law designed to protect the privacy of children, indirectly facilitates the attack. In order to bypass restrictions put in place due to the COPPA law, some children lie about their ages when registering, which not only increases the exposure for themselves but also for their non-lying friends.

Drawbacks of Existing System

This notice medical information about you may be used and disclosed and how you can get access to this information.It can describing all uses and disclosures of protected minor's information that the entity is permitted or required to make and a statement saying all other uses of the information must come with express authorization of the individual.

- Less security.
- Cannot able to identify who have tried to attack minor's attack based on geographical area where he is located.

- Need lack of time and individual attacker monitoring system to improve the security and privacy issues.

- Lack of accountability and transparency.

- Lot issues in censorship and data control management.

Proposed System

To recognize the importance of protecting the Internet privacy of minors (less than 18 years of age). Online Social Networks, in particular, take precautions to prevent third parties from using their services to discover and profile minors. These precautions include banning young children from joining, not listing minors when searching for users by high school or city, and displaying only minimal information in registered minors' public profiles, no matter how they configure their privacy settings.

Benefits Of Proposed System

Improved data privacy using k-SVM satisfies condition need in security and privacy both. It supports of the original minor's profile can be recovered from randomized transactions. We illustrate the practical utility of our method through some tradeoffs charts.

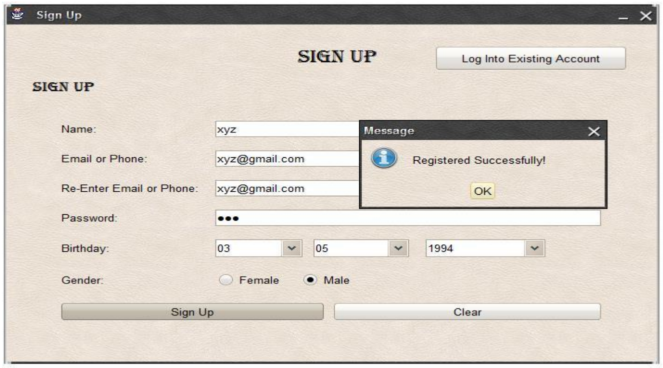
- Improved security.
- Better performance.
- Can able to find attacker list who have tried to hack minor's profile.
- Improved privacy for minor's profile and transparency.

Better accountability. Improved data control management on minor profile classification from hacker list.

Future Enhancement

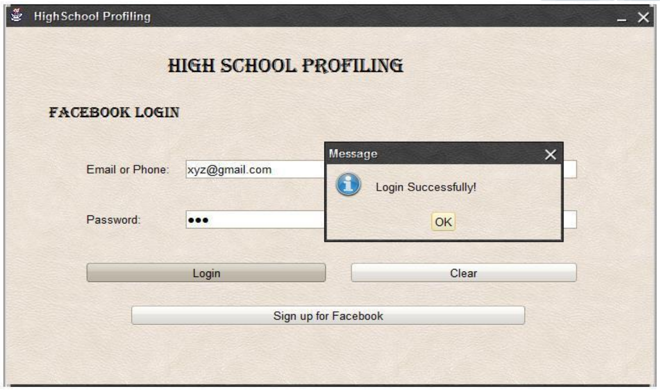
Social network information is now being used in ways for which it may have not been originally intended. In particular, increased use of smartphones capable of running applications which access social network information enable applications to be aware of a user's location and preferences. However, future models for exchange of this information require users to compromise their privacy and security. We present several of these privacy and security issues, along with our design and implementation of solutions for these issues. Our future work will allows location-based services to query without disclosing user identity or compromising users' privacy and security. We contend that it is important that such solutions be accepted as mobile social networks continue to grow exponentially.

V. RESULT AND DISCUSSION



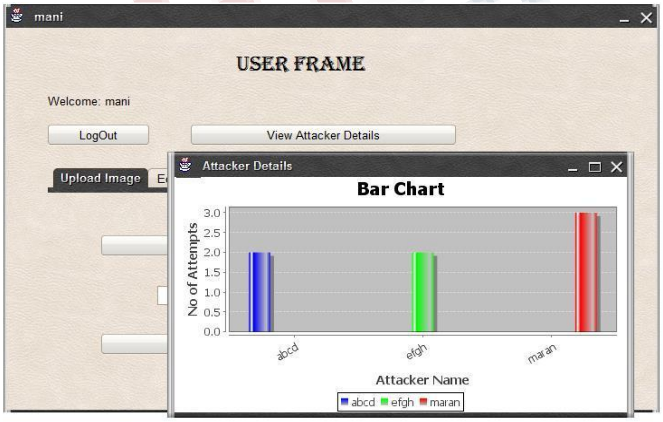
Name: xyz
Email or Phone: xyz@gmail.com
Re-Enter Email or Phone: xyz@gmail.com
Password: •••
Birthday: 03 05 1994
Gender: ○ Female ● Male

Registered Successfully!



Email or Phone: xyz@gmail.com
Password: •••

Login Successfully!



VI. CONCLUSION

In this work shown it is implemented how a privacy law for protecting children's privacy can inadvertently increase minor's exposure to third parties. The K-SVM takes precautions to prevent strangers from using their services to extensively profiles of minors. Here the consolidated and protected approach for minor not to revile lie about their ages, In this work with a precautionary measures the prediction of the real and fake data of a minor get in to the facebook For a given target high school, we described an attack of using an OSN to profile the current students in the high school. The attack finds the majority of the students in the school, and for each student build a profile that includes information that is not normally available to strangers, including current city, current school, high-school friends, and estimated birth year. Although the privacy law indirectly make the third party privacy problem for minors, We believe, however, that the laws must be carefully designed and consider leakages to hackers and duplicate profile creating minors.

REFERENCES

[1] Jose M. Such and member,IEEE, Natalia Criado: Resolving multi party privacy conflicts in social media. In proceeding of TKDE 2016: Security and privacy

[2]J. Becker and H. Chen: Measuring Privacy Risk in Online Social Networks. In Proceedings of W2SP 2009: Web 2.0 Security and Privacy, 2009.

[3] R. Dey, C. Tang, K. W. Ross, and N. Saxena. Estimating age privacy leakage in online social networks. In Proceedings of the IEEE INFOCOM 2012, Orlando, FL, USA, pages 2836–2840, 2012.

[4] A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel. You are who you know: inferring user profiles in online social networks. In Proceedings of the third ACM International Conference on Web Search and Data Mining, pages 251–260, 2010.

[5]K. Thomas, C. Grier, and D. M. Nicol. Unfriendly: multi-party privacy risks in social networks. In Proceedings of the 10th International Conference on Privacy enhancing technologies, pages 236–252,2010.
[6] B. Viswanath, A. Mislove, M. Cha, and K. P. Gummadi. On the evolution of user interaction in facebook.In Proceedings of the 2nd ACM workshop on Online Social Networks, pages 37–42, New York, NY,USA, 2009. ACM.