Privacy Protecting of Sensitive Information in Social Networking Media

G. Nagendra Kumar
Assistant Professor
Department of Computer Science and Engineering
K G Reddy College of Engineering and Technology, Hyderabad, India.

Abstract: Privacy is one of the major concerns when publishing or sharing social network data for social science research and business analysis. Recently, researchers have developed privacy models similar to k-anonymity to prevent node re-identification through structure information. However, even when these privacy models are enforced, an attacker may still be able to infer one's private information if a group of nodes largely share the same sensitive labels (i.e., attributes). In other words, the label-node relationship is not well protected by pure structure anonymization methods. Furthermore, existing approaches, which rely on edge editing or node clustering, may significantly alter key graph properties. In this paper, we define a k-degree-l-diversity anonymity model that considers the protection of structural information as well as sensitive labels of individuals. We had seen a novel anonymization methodology based on adding noise nodes. We implemented that algorithm by adding noise nodes into the original graph with the consideration of introducing the least distortion to graph properties. We here propose novel approach to reduce number of noise node so that decrease the complexity within networks. We implement this protection model in a distributed environment, where different publishers publish their data independently Most importantly, we provide a rigorous analysis of the theoretical bounds on the number of noise nodes added and their impacts on an important graph property. We conduct extensive experiments to evaluate the effectiveness of the proposed technique.
Keywords: Privacy, Online Social Network, Privacy protecting in SN, Sensitive information.

I. INTRODUCTION

Data mining refers to Knowledge Discovery in Databases. The data mining process is the extraction of information from various data sets and transform to an understandable manner. A social network is a social graph made up of actors such as individuals or organizations and connections. A social network service consists of a representation of each users, social links and variety of additional services. Most social network services provide means for users to interact over the Internet, such as e-mail and messaging. Social network sites are varied and they incorporate new information and communication tools.

The major drawbacks of social networks opens up the possibility of hackers to commit fraud and increases the risk of people falling prey to outline scams resulting in data or identity theft and potentially results in lost productivity. It refers to confidentiality of employer trade secrets and their private information. In order to provide security to social network users our algorithms issue anonymized views of the graph with significantly smaller information losses and analyze their privacy and communication complexity. Formally, in this social networks always represented as a graph, which we refer to as the social graph. The node of such a graph represents an actor and the edges represent ties between those actors.

II. RELATED WORK

A. Existing System

The current trend in the Social Network it not giving the privacy about user profile views. The method of data sharing or (Posting) has taking more time and not under the certain condition of displaying sensitive and non-sensitive data. There is no way to publish the Non sensitive data to all in social Network. It's not providing privacy about user profiles. Some mechanisms that prevent both inadvertent private information leakage and attacks by malicious adversaries.

B. Proposed System

Here, we extend the existing definitions of modules and we introduced the sensitive or non-sensitive label concept in our project. We overcome the existing system disadvantages in our project. We can publish the Non sensitive data to every-one in social Network. It's providing privacy for the user profiles so that unwanted persons not able to view your profiles. We can post sensitive data to particular peoples and same way we can post non-sensitive data to everyone like ads or job posts

III. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

1. User Module

In this module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first.

2. Information Loss

We aim to keep information loss low. In- formation loss in this case contains both structure information loss and label information loss. There are some non sensitive data's are Loss due to Privacy making so we can't send out full information to the public.

3.Sensitive Label Privacy Protection

There are who post the image to the online social network . if allow the people for showing the image it will display to his requesters it make as the sensitive to that user. Thesis is very useful to make sensitive data for the public.

IV. EXPERIMENTAL RESULT

Fig1. Login & Registration.

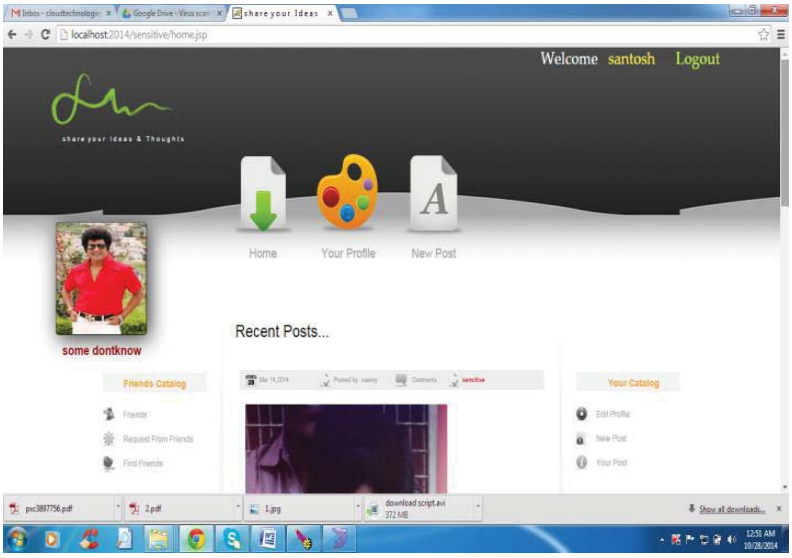

Fig2. Users Panel .

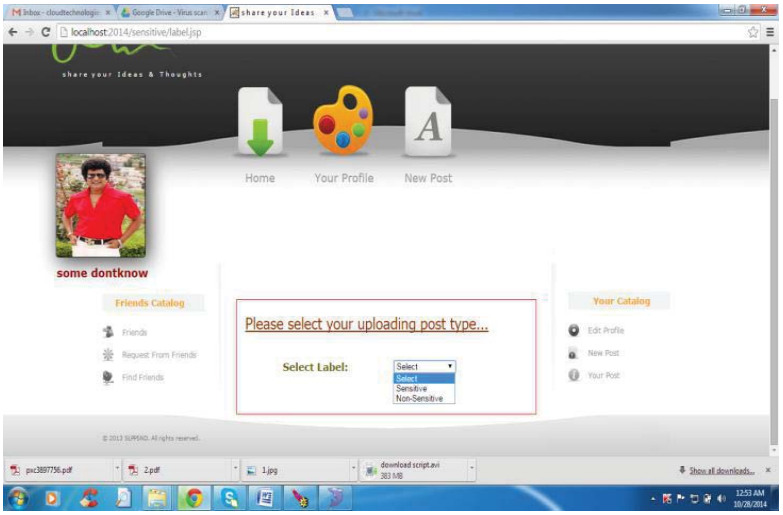

Fig3. Sensitive information

V. CONCLUSION

We propose a k-degree-l-diversity model for privacy preserving social network data publishing. We implement distinct K-degree, l-diversity and Anonymization. We design an algorithm to preserving privacy of user on social network. We are using heuristic search strategy that will search the input phase with minimum overhead. With give approximate answer within polynomial time. We give a rigorous analysis of the theoretical bounds on the minimum number of noise nodes added. Extensive experimental results demonstrate that the add minimum noise node AES algorithms and heuristic strategy can achieve a better result than the previous work using edge editing only and noise node adding attractive direction to study clever algorithms which can reduce the reduction of noise nodes with anonymization and diversity. Privacy is key matter when sharing social network data for organization and personal. It is necessary of today's large use of social network to provide privacy and security of private

information. We present new technique that will reduce noise nodes in our model Add minimum no of nodes & improve anonymization technique. We implement privacy-preserving approach. It is designed to help out these publishers publish an integrated data together to certification the security and privacy.

REFERENCES

[1] K. Le-Fevre, D. DeWitt, R. Ramakrishnan. Mondrian multidimensional k-anonymity In International Conference on Data Engineering 2006

[2] A. Meyerson and R. Williams. On the complexity of optimal k-anonymity CM Symposium on Principles of Database Systems 2004

[3] B.S. Hettich and C. Merz. UCI repository of machine learning databases, 1998

[4] P. Samarat,- Protecting respondent's privacy in micro data release IEEE Transactions on Knowledge and Data Engineering, 13, 2001.

[5] L. sweeney, achieving k-anonymity privacy protection using generalization and suppression. International journal on uncertainty, Fuzziness and knowledge based system, 2002.

[6] A.-L. Baraba´ si and R. Albert, "Emergence of Scaling in Random Networks," Science, vol. 286, pp. 509-512, 1999.

[7] Bruce Kapron, GautamSrivastava, S. Venkatesh -IEEE international Conference 2011, Social Network anonymization via Edge Addition.

[8] Benjamin C. M. Fung, Ke Wang, and Philip S.Yu, Fellow, IEEE Data Engineering 2007 AnonymizingClassication Data for Privacy Preservation.

[9] Ping Xiong, Tianqing Zhu management of e-Commerce and e Government (ICMeCG), 2012 Conference on An AnonymizationMethod Based on Tradeoff between Utility and Privacy for Data Publishing.

[10] Gionis A.; Tassa, T, IEEE Knowledge and data engineering 2009.K anonymization with minimal loss of information.

[11] Shapiro, S S. (SysCon) IEEE Knowledge and data engineering 2012, Situating Anonymization within Privacy risk model