ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

A strong and efficient privacy and security guarantee using CACHET

ADDANKI NAGESHWAR RAO[1], B.KAMESWARA RAO[2]

M.Tech [Scholar], Department of CSE, Vizag Institute of Technology, Visakhapatnam, AP, India [1]

HOD, Department of CSE, Vizag Institute of Technology, Visakhapatnam, AP, India [2]

Abstract: This project is motivated by the recognition of the need for a finer grain and more personalized privacy in data publication of social networks. We propose a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in users' profiles. An individual user can select which features of her profiles she wishes to conceal. The social networks are modelled as graphs in which users are nodes and features are labels. Labels are denoted either as sensitive or as non-sensitive. We treat node labels both as background knowledge an adversary may possess, and as sensitive information that has to be protected. We present privacy protection algorithms that allow for graph data to be published in a form such that an adversary who possesses information about a node's neighbourhood cannot safely infer its identity and its sensitive labels. To this aim, the algorithms transform the original graph into a graph in which nodes are sufficiently indistinguishable. The algorithms are designed to do so while losing as little information and while preserving as much utility as possible. We evaluate empirically the extent to which the algorithms preserve the original graph's structure and properties. We show that our solution is effective, efficient and scalable while offering stronger privacy guarantees than those in previous research.

Keywords: Privacy, CACHET, protection, social networking

I. INTRODUCTION

The publication of social network data entails a privacy threat for their users. Sensitive information about users of the social networks should be protected [1-4]. The challenge is to devise methods to publish social network data in a form that affords utility without compromising privacy. Previous research has pro-posed various privacy models with the corresponding protection mechanisms that prevent both inadvertent private information leakage and attacks by malicious adversaries. These early privacy models are mostly concerned with identity and link disclosure[5]. The social networks are modeled as graphs in which users are nodes and social connections are edges. The threat definitions and protection Sensitive Label Privacy Protection on Social Network Data mechanisms leverage structural properties of the graph[6-8]. This project is motivated by the recognition of the need for a finer grain and more personalized privacy. Users entrust social networks such as Facebook and LinkedIn with a wealth of personal information such as their age, address, current location or political orientation. We refer to these details and messages as features in the user's profile. We propose a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in users' profiles. An individual user can select which features of her profile she wishes to conceal.

The social networks are modeled as graphs in which users are nodes and features are labels. Labels are denoted either as sensitive or as non-sensitive. Each node in the graph represents a user, and the edge between two nodes represents the fact that the two persons are friends. Labels annotated to the nodes show the locations of users. Each letter represents a city name as a label for each node. Some individuals do not mind their residence being known By the others, but some do, for various reasons. In such case, the privacy of their labels should be protected at data release. Therefore the locations are either sensitive or non-sensitive. The privacy issue arises from the disclosure of sensitive labels. One might suggest that such labels should be simply deleted. Still, such a solution would present an incomplete view of the network and may hide interesting statistical information that does not threaten privacy[6]. A more sophisticated approach consists in releasing information about sensitive labels, while ensuring that the identities of users are protected from privacy threats [7]. We consider such threats as neighborhood attack, in which adversary friends out sensitive information based on prior knowledge of the number of neighbors of a target node and the labels of these neighbors.

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. Problems on existing system are

a) There is no way to publish the Non sensitive data to all in social Network.
b) It’s not providing privacy about user profiles.

Some mechanisms that prevent both inadvertent private information leakage and attacks by malicious adversaries.

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 isadvantages in our project.

a) We can publish the Non sensitive data to everyone in social Network.
b) It's providing privacy for the user profiles so that unwanted persons not able to view your profiles.
c) We can post sensitive data to particular peoples and same way we can post non-sensitive data to everyone like ads or job posts.

II. DATA FLOW DIAGRAM OF THE PROPOSED METHOD

DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system.

The representation of the User, Administrator and the Publisher are given in the Fig.1 through Fig.3. The DFD helps to understand the structure of the system.

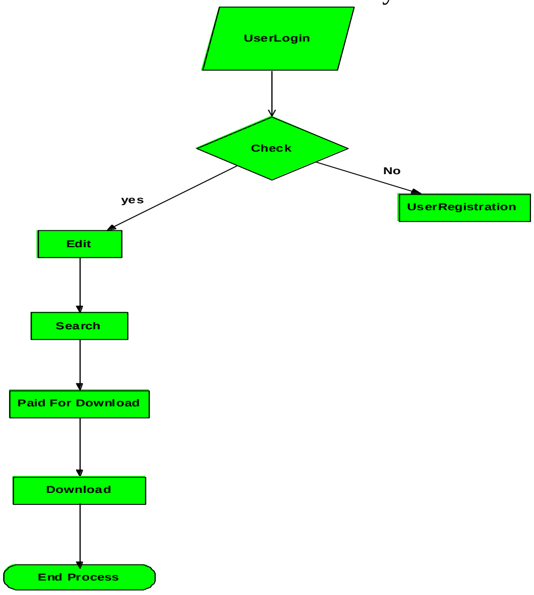


Fig.1: User

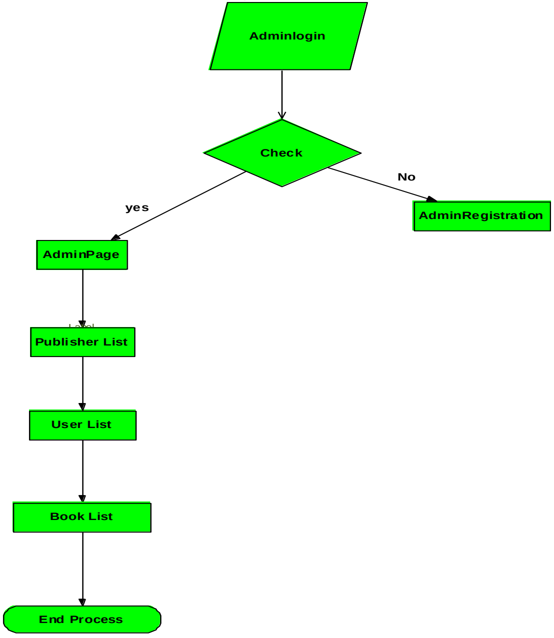


Fig.2: Admin

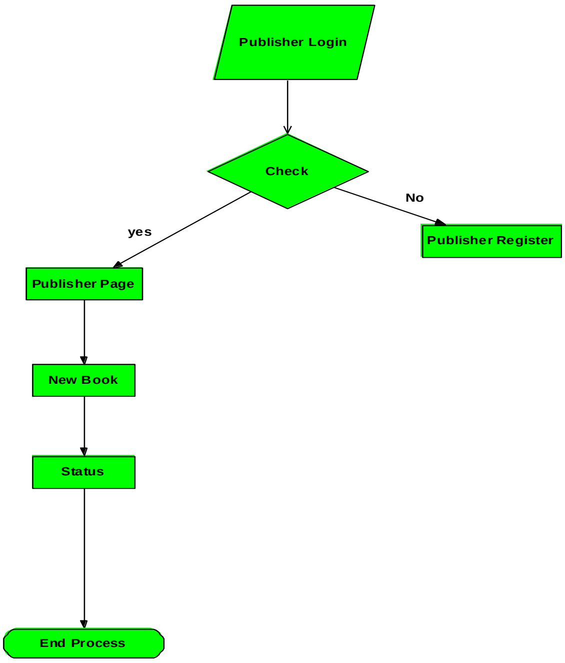


Fig.3: Publisher

III.SYSTEM STUDY

The description of the system study is given in this section

FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

i. ECONOMICAL FEASIBILITY
ii. TECHNICAL FEASIBILITY
iii. SOCIAL FEASIBILITY

ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system

IV. RESULTS

INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

a) What data should be given as input?

b) How the data should be arranged or coded?

c) The dialog to guide the operating personnel in providing input.

d) Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

i) Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

ii) It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

iii) When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements. Select methods for presenting information. Create document, report, or other formats that contain information produced by the system. The output form of an information system should accomplish one or more of the following objectives.

a) Convey information about past activities, current status or projections of the

b) Future.

c) Signal important events, opportunities, problems, or warnings.

d) Trigger an action.

e) Confirm an action.

The screen shots of the proposed representation is given in Fig.4 through 8.

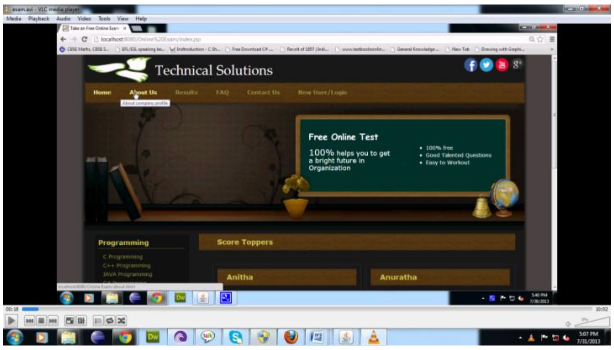
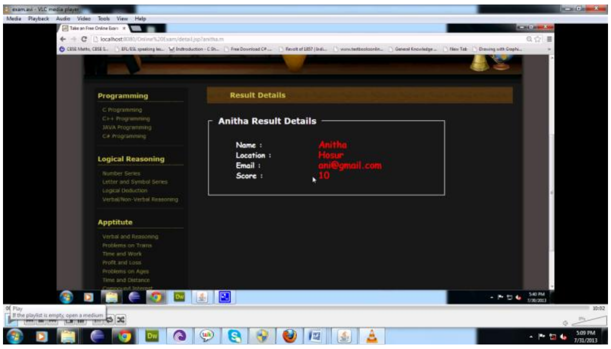


Fig.4: Home Screen

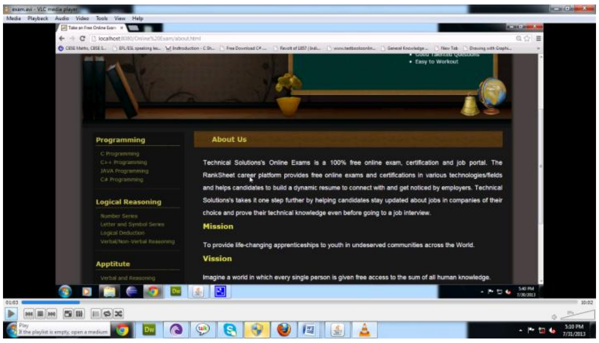


Anitha Result Details

Name : Anitha
Location : Hosur
Email : ani@gmail.com
Score : 10

If the playlist is empty, open a medium

Fig.5: Score topper's screen



About Us

Technical Solutions's Online Exams is a 100% free online exam, certification and job portal. The RankSheet career platform provides free online exams and certifications in various technologies/fields and helps candidates to build a dynamic resume to connect with and get noticed by employers. Technical Solutions's takes it one step further by helping candidates stay updated about jobs in companies of their choice and prove their technical knowledge even before going to a job interview.

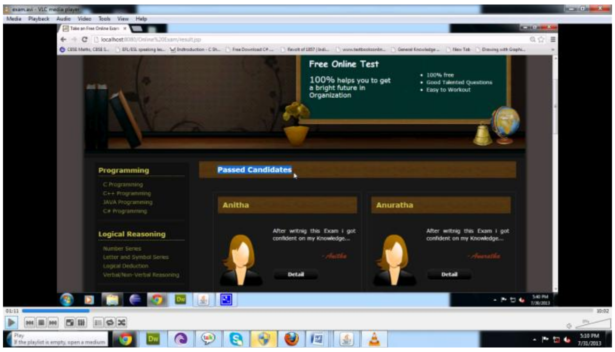
Mission

To provide life-changing apprenticeships to youth in undeserved communities across the World.

Vission

Imagine a world in which every single person is given free access to the sum of all human knowledge.

Fig.6: About us



Passed Candidates

Anitha

After writnig this Exam i got confident on my Knowledge...

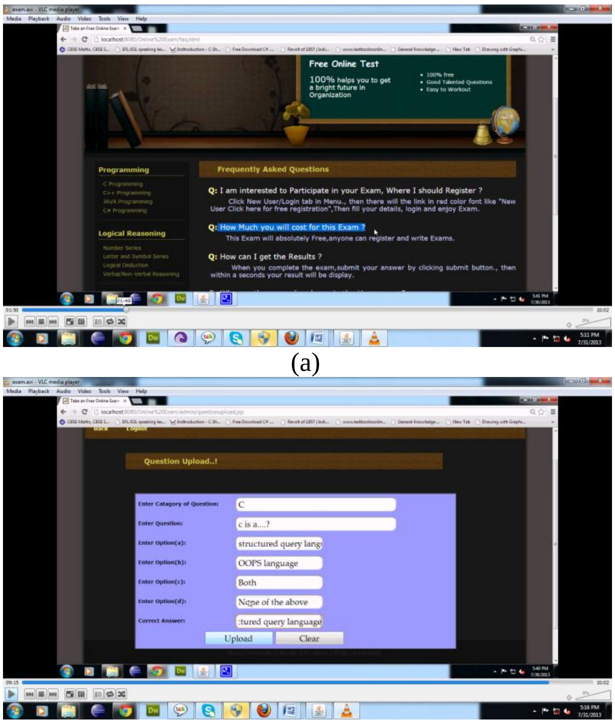
-Anitha

Anuratha

After writnig this Exam i got confident on my Knowledge...

-Anuratha

Fig.7: Passed candidates



(a)

Frequently Asked Questions

Q: I am interested to Participate in your Exam, Where I should Register ?
Click New User/Login tab in Menu., then there will the link in red color font like "New User Click here for free registration",Then fill your details, login and enjoy Exam.

Q: How Much you will cost for this Exam ?
This Exam will absolutely Free,anyone can register and write Exams.

Q: How can I get the Results ?
When you complete the exam,submit your answer by clicking submit button., then within a seconds your result will be display.

(b)

Question Upload..!

Enter Catagory of Question: C
Enter Question: c is a....?
Enter Option(a): structured query lang
Enter Option(b): OOPS language
Enter Option(c): Both
Enter Option(d): None of the above
Correct Answer: :tured query language

Fig.8 (a&b): Questions Screens

V. Conclusion

Sensitive Label Privacy Protection on Social Network Data we have investigated the protection of private label information in social network data publication. We consider graphs with rich label information, which are categorized to be either sensitive or non-sensitive. We assume that adversaries possess prior knowledge about a node's degree and the labels of its neighbors, and can use that to infer the sensitive labels of targets. We suggested a model for attaining privacy while publishing the data, in which node labels are both part of adversaries' background knowledge and sensitive information that has to be protected. We accompany our model with algorithms that transform a network graph before publication, so as to limit adversaries' confidence about sensitive label data. Our experiments on both real and synthetic data sets confirm the effectiveness, efficiency and scalability of our approach in maintaining critical graph properties while providing a comprehensible privacy guarantee.

References

[1] Shirin Nilizadeh, Sonia Jahid, Prateek Mittal, Nikita Borisov, and ApuKapadia, "Cachet: A Decentralized Architecture for Privacy Preserving Social Networking with Caching," In *Proceedings of The 8th ACM International Conference on Emerging Networking Experiments and Technologies (CoNEXT '12)*, pp. 337–348, Nice, France, December 10–13, 2012.

[2] Sonia Jahid, Shirin Nilizadeh, Prateek Mittal, Nikita Borisov, and ApuKapadia, "DECENT: A Decentralized Architecture for Enforcing Privacy in Online Social Networks," In *Proceedings of the 4th IEEE International Workshop on Security and Social Networking (SESOC '12)*, pp. 326–332, Lugano, Switzerland, March 19, 2012.

[3] Shirin Nilizadeh, Naveed Alam, Nathaniel Husted, and Apu Kapadia, "Pythia: A Privacy Aware, Peer-to-Peer Network for SocialSearch," In *Proceedings of the 2011 ACM Workshop on Privacy in the Electronic Society (WPES '11)*, pp. 43–48, Chicago, Illinois, October 17, 2011.

[4] Ruj Akavipat, Mahdi N. Al-Ameen, Apu Kapadia, Zahid Rahman, Roman Schlegel, and Matthew Wright, "ReDS: A Framework for Reputation-Enhanced DHTs", *IEEE Transactions on Parallel and Distributed Systems (IEEE TPDS)*, Volume 25, Issue 2, pp. 321–331 (February 2014). Available as IEEE online preprint, 2013

[5] Man Ho Au, Patrick P. Tsang, and Apu Kapadia, "PEREA: Practical TTP-Free Revocation of Repeatedly Misbehaving Anonymous Users," *ACM Transactions on Information and System Security (ACM TISSEC)*, Volume 14, Issue 4, Article 29, 34 pages (December 2011). (Extends our CCS '08 conference paper, which was *Runner-up for PET Award 2009: Outstanding Research in Privacy Enhancing Technologies*)

[6] Patrick P. Tsang, Apu Kapadia, Cory Cornelius, and Sean W. Smith, "Nymble: Blocking Misbehaving Users in Anonymizing Networks," *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, Volume 8, Number 2, pp. 256–269 (March–April 2011).

[7] Minho Shin, Cory Cornelius, Dan Peebles, Apu Kapadia, David Kotz, and Nikos Triandopoulos, "AnonySense: A System for Anonymous Opportunistic Sensing," *Journal of Pervasive and Mobile Computing (PMC)*, Volume 7, Issue 1, pp. 16–30 (February 2011).

[8] Patrick P. Tsang, Man Ho Au, Apu Kapadia and Sean W. Smith, "BLAC: Revoking Repeatedly Misbehaving Anonymous Users Without Relying on TTPs," *ACM Transactions on Information and System Security (ACM TISSEC)*, Volume 13, Issue 4, Article 39, 33 pages (December 2010).

DOI 10.17148/IJARCCE