DYNAMIC TEXT BLOCKING IN SOCIAL NETWORKS FOR USER EXPERIENCE

V.R.Sridevi[#1], G.Sathya[#2]., ME
[#1]Pg Scholar, [#2]Associate Professor & Oxford Engg College
Department of Computer Science and Engineering & Oxford Engineering, Trichy, Tamilnadu, India
[1]sriderviprasanna85@gmail.com, [2]sathya161088@gmail.com@gmail.com

ABSTRACT

Online social systems have become an important part of everyday life. While initial examples were used to share personal content with friends more and more online social systems are also used to do business. Unfortunately, privacy concerns raised in the recommendation process impede the expansion of OSN user's friend circle. Some OSN users refuse to disclose their identities and their friend's information to the public domain. Indeed, today OSNs provide very little support to prevent unwanted messages on user walls. In order to avoid this problem, in the proposed system the dynamic blocking algorithm has been implemented which automatically blocks the unwanted text message and in the classification methods using the supervised methods the decision tree has been used. Using the decision tree, it creates the more number of categories, and it stores more data under this category.

KEYWORDS: Recommended systems, social trust, matrix factorization, implicit trust, collaborative filtering.

INTRODUCTION

Online Social Network Systemhave been widely used to provide users with high-quality personalized recommendations from a large volume of choices. Robust and accurate recommendations are important in e-commerce operations (e.g., navigating product offerings, personalization, improving customer satisfaction), and in marketing (e.g., tailored advertising, segmentation, cross-selling). Collaborative filtering (CF) is one of the majorityaccepted techniques to realize a recommenderscheme. The idea of CF is that users with similar preferences in the past are likely to favor the same items (e.g., movies, music, books, etc.) in the future. CF has also been applied to tasks besides item recommendations, in domains such as image processing and bioinformatics. However, CF suffers from two well known issues: Data Sparsity and Cold start. The former issue refers to the fact that users usually rate only a small portion of items, while the latter indicates that new users only give a few ratings (a.k.a. cold-start users). Both issues severely degrade the efficiency of a recommender system in modeling user preferences and thus the accuracy of predicting a user's rating for an unknown item.

One possible explanation is that these trust-based models focus too much on the utility of user trust but ignore the influence of item ratings themselves. Toinvestigate this phenomenon, an empirical trust analysis based on four real-world data sets has been conducted (Film Trust, Epinions, Flixster and Ciao). Three important observations emerge. First, trust information is also very sparse, yet complementary to rating information.

The third observation further indicates a similar conclusion with in-coming trusting neighbours (i.e., trusters). The implication is that existing trust-based models may not work well if there exists only trust-alike relationships. Given that very littlebelief networks live, it is enhanced to have anadditional general trust-based reproduction that can operates well on both trust and trust-alike relationships. These observations motivate us to consider both explicit and implicit influence of item ratings and of user trust in a unified trust-based model. The influence can be explicit— real values of ratings and trust or implicit who rates what (for ratings) and who trusts whom (for trust). The implicit influence of ratings has been demonstrated useful in providing accurate recommendations. It will later show that implicit trust can also provide added value over explicit trust.

In addition, itfurtherconsiders the influence of user trust (including trustees and trusters) on the rating prediction for an active user. To the author's knowledge, our first work is to extend SVD++ with social trust information. Specifically, on one hand the implicit influence of trust (who trusts whom) can be naturally added to the SVD++ model by extending the user modeling. On the other hand, the explicit influence of trust (trust values) is used to constrain that user-specific vectors should conform to their social trust relationships. This ensures that user-specific vectors can be educated from their beliefin sequence even if a few or no ratings are given. In this way, the concerned issues can be better alleviated. Our method is novel for its consideration of both the explicit and implicit influence of item ratings and of user trust. In addition, a weighted regularization technique is used to help avoid over-fitting for model learning. The experimental results on the four real world data sets demonstrate that our approach works significantly better than other trust-based counterparts as well as high-performing ratings-only models (10 approaches in total) in terms of predictive accuracy, and is more capable of coping with the cold-start situations.

RELATED WORKS

In [1] Hao Ma, Haixuan Yang, Michael R. Lyu, Irwin King et al presents Data Sparsity, scalability and prediction quality have been documented as the three most critical challenges that every collaborative filtering algorithm or recommender system con- fronts. Many existing approaches to recommender systems can neither handle very huge datasets nor easily deal with users who have made very little ratings or even none at all. Moreover, traditional recommender systems guess that all the users are independent and identically distributed; this assumption ignores the social interactions or connections among users. In view of the exponential growth of in sequence generated by online social networks, social network analysis is becoming important for many Web applications. Following the intuition that a person's social network will affect personal behaviors on the Web, this paper proposes a factor examination approach based on probabilistic matrix factorization to explain the data Sparsity and poor prediction correctness problems by employing both users social network in sequence and ranking records.

In [2] Jianke Zhu, Hao Ma, Chun Chen, and Jiajun Bu et al presents The most critical challenge for the recommendation system is to achieve the high prediction quality on the large scale sparse data donatedby the users. In this project,a novel approach has been presented to the social recommendation trouble, which takes the advantage of the graph Laplacian regularization to capture the underlying social relationship among the users. Different from the previous approaches that are based on the conventional gradient tumble optimization itformulates the presented graph Laplacian regularized social recommendation problem into a low-rank semi definite program, which is able to be competently solved by the quasi-Newton algorithm. It does haveto conduct the experiential evaluation on a large scale dataset of high Sparsity, the talented experimental results shows that our process is very effective and proficient for the social recommendation task.

In [3] Bo Yang, Yu Lei, Dayou Liu, Jiming Liu et al presents To accurately and aggressivelysupply users with their potentially interested information or services is the chief task of a recommender system. Collaborative filtering is one of the most widely adopted recommender algorithms, whereas it is suffering the issues of data Sparsity and cold start that will sternly degrade excellence of recommendations. To address such issues, this article proposes a novel method, trying to improve the performance of collaborative filtering recommendation by means of elaborately integrating twofold sparse information, the conventional rating data given by users and the social trust network amongst the same users. It is a model-based technique adopting matrix factorization practice to map users into low-dimensional covert feature spaces in terms of their convictionaffiliation, aiming to reflect usersmutual influence on their own opinion more reasonably.

In [4] Mohsen Jamali, Martin Ester et al presents Collaborative filtering is the most accepted approach to build recommender systems and has been successfully working in lots of applications. However, it cannot make recommendation for so-called cold start users that have rated only a very littlenumeral of items. In addition, these methods do not identify how confident they are in their recommendations. Trust-based recommendation methods assume the additional knowledge of a trust network among users and can better deal with cold start users, since users only need to be simply linked to the trust network. On the other hand, the Sparsity of the user article ratings forces the trust based approach to believe ratings of circuitous neighbours that are only weakly trusted, which may decrease its precision. In order to find a good trade, a random walk reproduction combines the trust-based approach and the collaborative filtering approach for recommendation. The random walk model allows us to define and to determine the assurance of a recommendation.

In [5] GuibingGuo, Jie Zhang, and Daniel Thalmann et al presents Providing high superiority recommendations is imperative for online systems to support users who face a vast number of choices in productionby successful selection of decisions. Collaborative filtering is a widely conventional technique to provide recommendations based on ratings of similar users. But it suffers from several issues like data Sparsity and cold start. To address these issues, in this paper, recommending a straightforward but effective method, namely “Merge”, to incorporate social trust information (i.e. trusted neighbors overtly specified by users) in providing recommendation. More specially, ratings of a users trusted neighbours are compound to represent the preference of the user and to find alike other users for generating recommendations. Experimental results based on these real data sets show that this method is more effective than other approaches, both in accuracy and coverage of recommendations.

PROPOSED SYSTEM

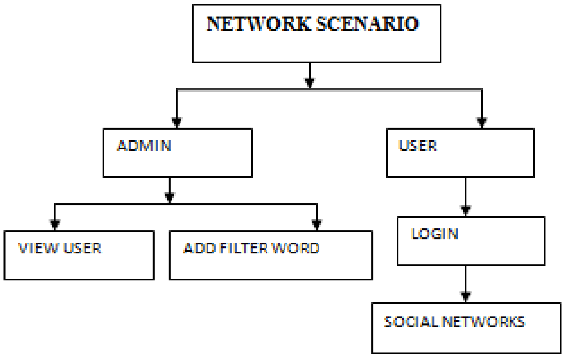
In the plannedcollection, a novel trust-based recommendation model tonormalize with user trust and item ratings, term Trust SVD is used. Our approach builds on top of a state-of the-art model SVD++ during which both the explicit and inherent influence of user–item ratings are concerned to generate predictions. In addition, further believe the influence of user trust (including trustees and trusters) on the rating prediction for avigorous user. To the authors knowledge, our first work is to extend SVD++ with social trust information. Specifically, on one hand the implicit influence of trust (who trusts whom) can be naturally added to the SVD++ model by extending the user modeling. On the other hand, the explicit influence of trust (trust values) is used to restrain that user-specific vectors should be traditional to their social trust relationships. This ensures that user-specific vectors can be educated from their faithin sequence even if a few or no ratings are given. In this way, the concerned issues can be better alleviated. Our technique is the novel fordeliberation of both the explicit and implicit pressure of item ratings and of user trust. In addition, a weighted-regularization method is used to assistevade over-fitting for model learning.

MODULE SPECIFICATION

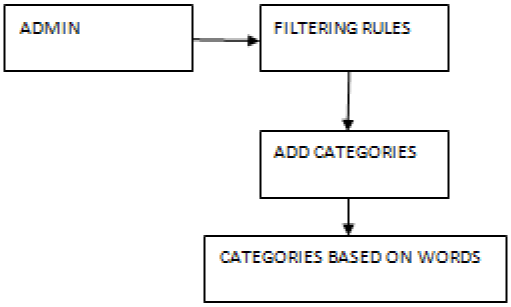
- Network scenario
- Filtering rules
- Online setup assistant for FRS thresholds
- Blacklists
- Blocked unwanted message
- Relative frequency
- Mail notification

NETWORK SCENARIO

Given the social network scenario, creators may also be identified by exploitin sequence on their social graph. This imply to state conditions on type, depth and trust values of the relationship(s) creators should be involved in order to pertain them the particular rules. All these options are formalized by the conception of creator specification, defined as follows.



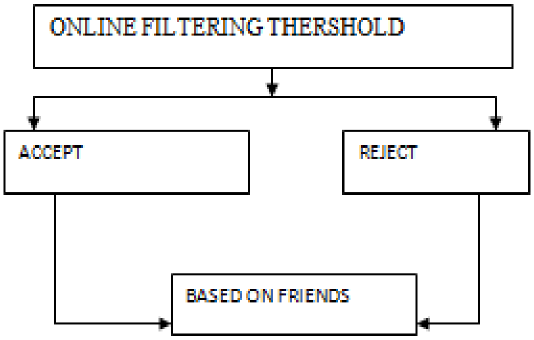
FILTERING RULES



In defining the language for FRs requirement, our estimationshould influence a message filtering decision. First of all, like OSNs in everyday life, the matching message may have assorted meanings and relevance based on who writes it. As a corollary, FRs should allow users to state constraints on message creators. Creators on which a FR applies can be selected on the basis of several different criteria; one of the most relevant is by striking conditions on their profile's attributes. In such a way it is, for occurrence, probable to describe rules applying only to young creators or to creators with a given religious/political view.

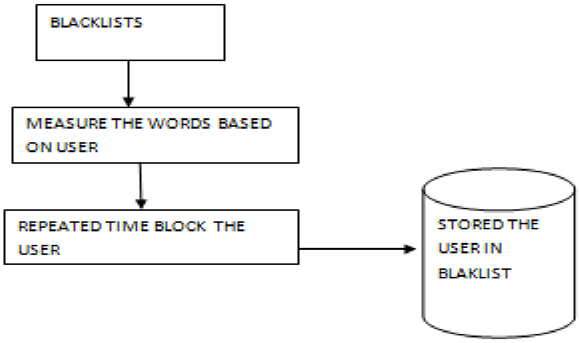
ONLINE FILTERING THERSHOLD

As mentioned in the previous section,lecture to the problem of location thresholds to filter rules, by conceiving and implement within FW, an Online Setup Assistant (OSA) practice is used. OSA presents the user with a set of messages,for each meaning, the user tells the classification(the decision) to accept or reject the message. The collection and processing of user decisions on an adequate set of messages dispersed over all the classes allows computing customized thresholds in place of the user approach in accepting or rejecting convinced contents.



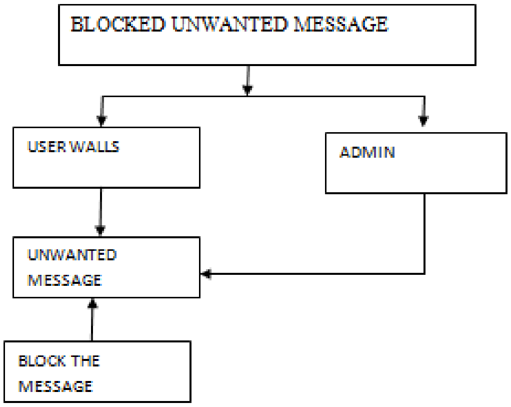
BLACKLISTS

Anaddedconstituent of our scheme is a BL equipment to evade messages from undesired creators, sovereign from their contents. BLs is directly managed by the organization, which should be able to determine who are the users to be inserted in the BL and to decide when user's retention in the BL is finished. To develop flexibility, a sequenceis given to the system through a set of rules, hereafter called BL rules. Such rules are not defined by the SNM; therefore they are not destined as general high level directives to be applied to the entire community. Rather, then decide to let the users themselves, i.e., the wall's owner to identify BL rules adaptable who has to be ineligible from their walls and for how long. Therefore, a user might be debarred from a wall, by, at the same time, being clever to post in other walls.


BLACKLISTS
MEASURE THE WORDS BASED ON USER
REPEATED TIME BLOCK THE USER
STORED THE USER IN BLAKLIST

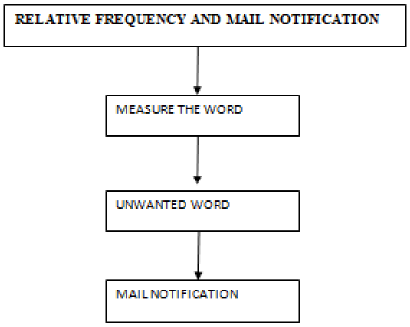
BLOCKED UNWANTED MESSAGE

Similar to FRs, our BL rules produce the wall owner able to classify users to be infertile according to their profiles as well as their relationships in the OSN. Therefore, by means of a BL law, wall owners are able to ban the users from their walls they do not honestlyknow (i.e., with which they have only roundabout relationships), or users that are friend of a known person as they might have a bad estimation of this person. This banning can be adopted for ahesitating time period or for a precise time window. Moreover, banning criteria may also take into explanation users' behavior in the OSN. More precisely, among possible information denoting the users bad performance it focus on two main measures. The first is connected to the principle that if within a given time interval a user has been inserted into a BL for several times, say greater than a given threshold, he/she might merit to stay in the BL for one more while, as his/her behavior is not improved. This mechanism is normal for those users that have been previously inserted in the measured BL at least one time.



RELATIVE FREQUENCY

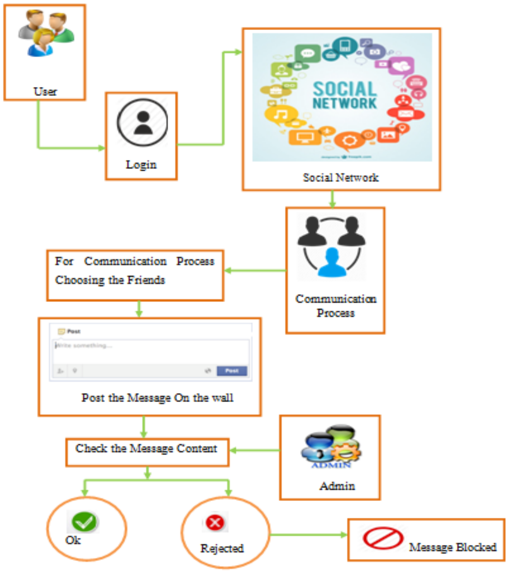
In difference, to catch thenovel bad behaviors, use the Relative Frequency (RF) that let the system to detect those users whose messages persist to fail the FRs. The two measures can be multiply either locally, that is, by in view of only the messages and/or the BL of the user specifying the BL rule or worldwide, that is, by allowing for all OSN users walls and/or BLs.



MAIL NOTIFICATION

In the mail contribution it develop the structure by creating aexample randomly notifying a message system that should in its place be blocked, or detecting modifications to profile attributes that have been made for the only reason of defeat the filtering organization. Automatically user will get a mail notification.

ARCHITECTURE DIAGRAM


User
Login
SOCIAL NETWORK
Social Network
Communication Process
For Communication Process Choosing the Friends
Post
Post the Message On the wall
Check the Message Content
ADMIN
Admin
Ok
Rejected
Message Blocked

RECOMMENDATION ALGORITHM

A recommenderarrangement or a recommendation structure (sometimes replacing "system" with a synonym such as platform or engine) is a subclass of in sequence filtering system that seeks to envisage the "rating" or "preference" that a user would furnish to an item.A recommender systemor a recommendation system (sometimes replacing "system" with a synonym such as platform or engine) is a subclass of information filtering organization that seeks to predict the "rating" or "preference" that a user would give to an item. Recommender systems have become increasingly popular in new years, and are utilized in a variety of areas counting movies, music, news, books, research articles, search queries, social tags, and products in universal.

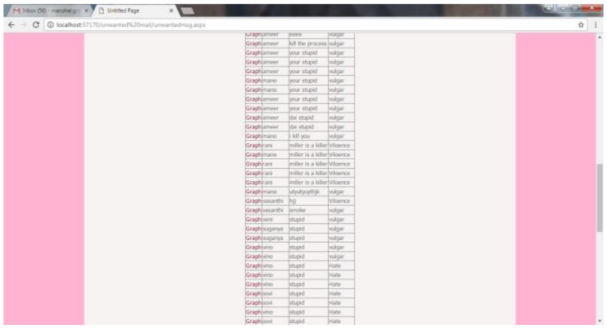
RATE PREDICATION ALGORITHM

Following are the example of cases where the data investigation chore is Prediction−suppose the marketing manager needs to predict how much a given customer will expend during the sales at his company. In this example it is bothered to predict a numeric value. Therefore the data investigation task is an example of numeric prediction. In this case, a sculpt or a predictor will be constructed that predicts a continuous-valued-function or prearrangedworth.

With the assist of the bank loan application which has been discussed above, let us appreciate the operation of classification. The Data Classification process includes two steps –

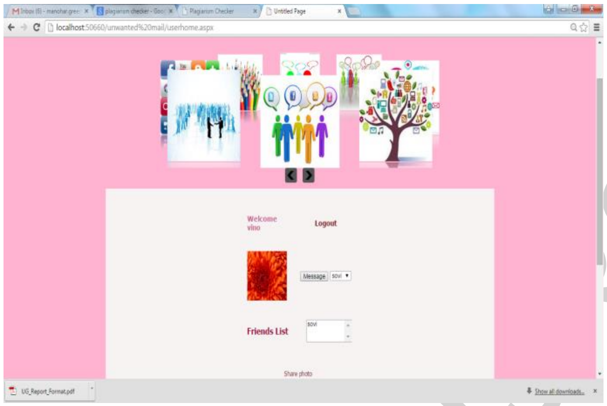
- Building the Classifier
- Model Using Classifier for Classification

OUTPUT RESULT



localhost:57170/unwanted%20mail/unwantedmsg.aspx

Graph	ameer	eeee	vulgar
Graph	ameer	kill the process	vulgar
Graph	ameer	your stupid	vulgar
Graph	ameer	your stupid	vulgar
Graph	ameer	your stupid	vulgar
Graph	mano	your stupid	vulgar
Graph	mano	your stupid	vulgar
Graph	ameer	your stupid	vulgar
Graph	ameer	your stupid	vulgar
Graph	ameer	dai stupid	vulgar
Graph	ameer	dai stupid	vulgar
Graph	mano	i kill you	vulgar
Graph	rani	miller is a killer	Viloence
Graph	mano	miller is a killer	Viloence
Graph	rani	miller is a killer	Viloence
Graph	rani	miller is a killer	Viloence
Graph	rani	miller is a killer	Viloence
Graph	mano	utyutyuythjk	vulgar
Graph	vasanthi	hjj	Viloence
Graph	vasanthi	smoke	vulgar
Graph	veni	stupid	vulgar
Graph	suganya	stupid	vulgar
Graph	suganya	stupid	vulgar
Graph	vino	stupid	vulgar
Graph	vino	stupid	vulgar
Graph	vino	stupid	Hate
Graph	vino	stupid	Hate
Graph	vino	stupid	Hate
Graph	sovi	stupid	Hate
Graph	sovi	stupid	Hate
Graph	vino	stupid	Hate
Graph	sovi	stupid	Hate



localhost:50660/unwanted%20mail/userhome.aspx

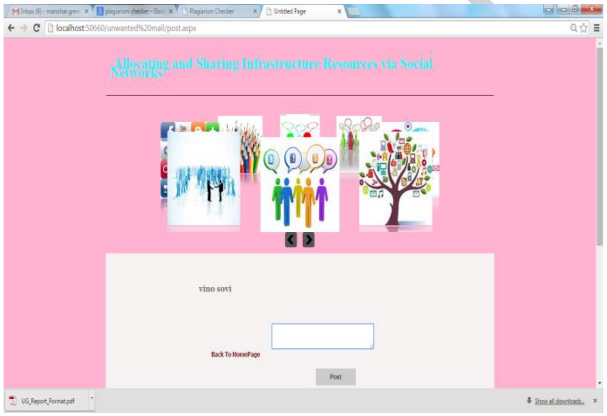
Welcome vino

Logout

Message | sovi

Friends List | sovi

Share photo



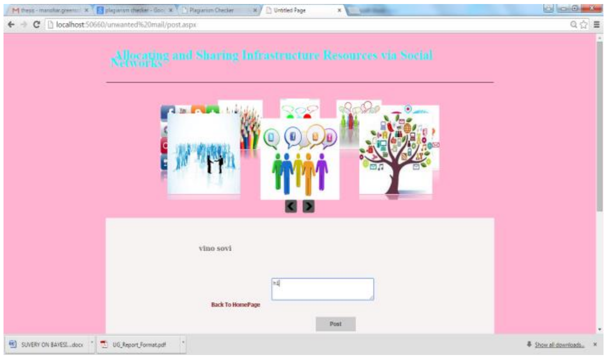
localhost:50660/unwanted%20mail/post.aspx

Allocating and Sharing Infrastructure Resources via Social Networks

vino sovi

Back To HomePage

Post



localhost:50660/unwanted%20mail/post.aspx

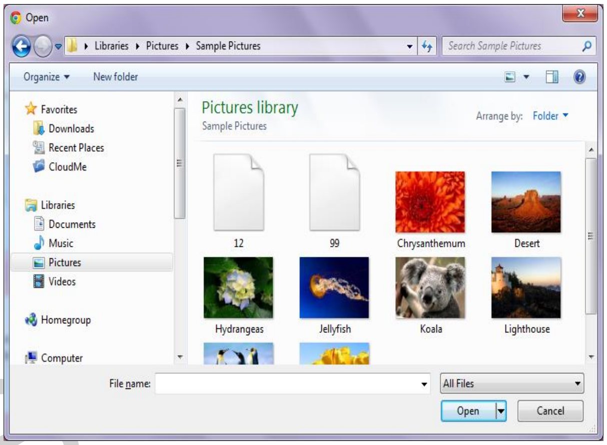
Allocating and Sharing Infrastructure Resources via Social Networks

vino sovi

hi

Back To HomePage

Post



Open

Libraries ▸ Pictures ▸ Sample Pictures

Search Sample Pictures

Organize ▾ New folder

Favorites, Downloads, Recent Places, CloudMe, Libraries, Documents, Music, Pictures, Videos, Homegroup, Computer

Pictures library

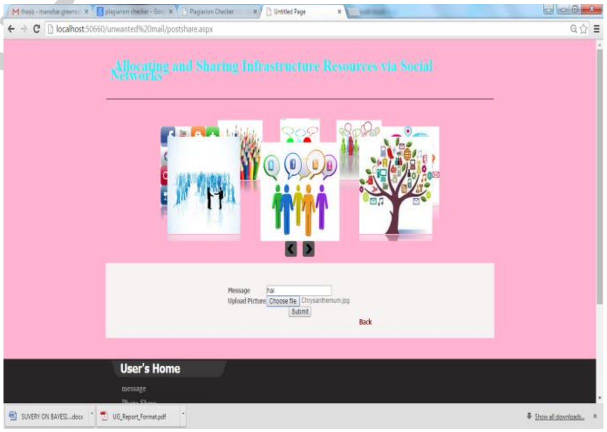
Sample Pictures

Arrange by: Folder ▾

12, 99, Chrysanthemum, Desert, Hydrangeas, Jellyfish, Koala, Lighthouse

File name: | All Files

Open | Cancel



localhost:50660/unwanted%20mail/postshare.aspx

Allocating and Sharing Infrastructure Resources via Social Networks

Message: hai

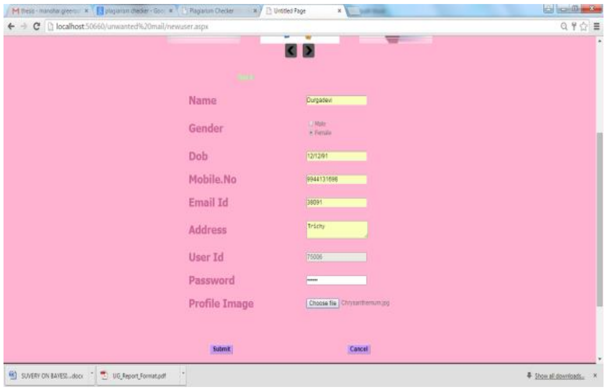
Upload Picture: Choose file Chrysanthemum.jpg

Submit

Back

User's Home

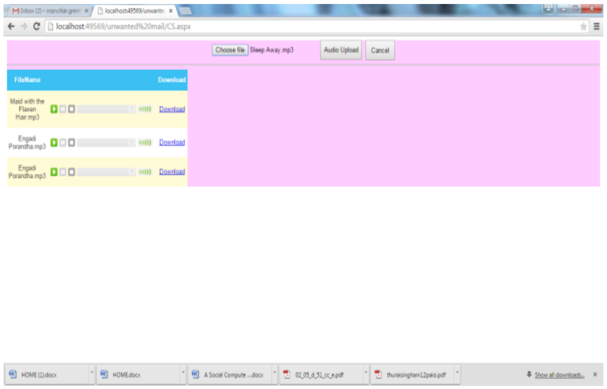
message



localhost:50660/unwanted%20mail/newuser.aspx

Name	Durgadevi
Gender	○ Male ● Female
Dob	12/12/91
Mobile.No	9944131696
Email Id	38091
Address	Trichy
User Id	75006
Password	******
Profile Image	Choose file Chrysanthemum.jpg

Submit | Cancel

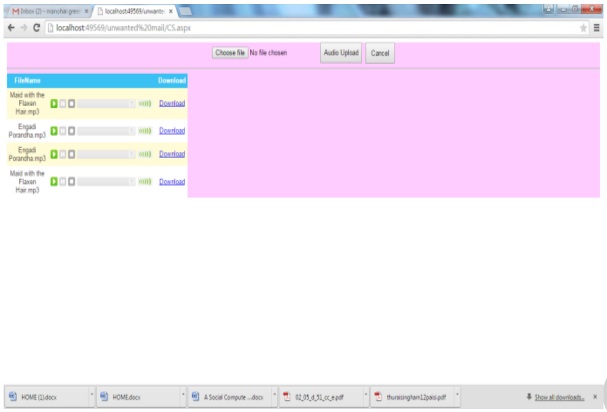


localhost:49569/unwanted%20mail/CS.aspx

Choose file Sleep Away.mp3

FileName	Download
Maid with the Flaxen Hair.mp3	Download
Engadi Porandha.mp3	Download
Engadi Porandha.mp3	Download

HOME (1).docx | HOME.docx | A Social Compute ...docx | 02_05_d_51_cc_e.pdf | thuraisingham12paisi.pdf

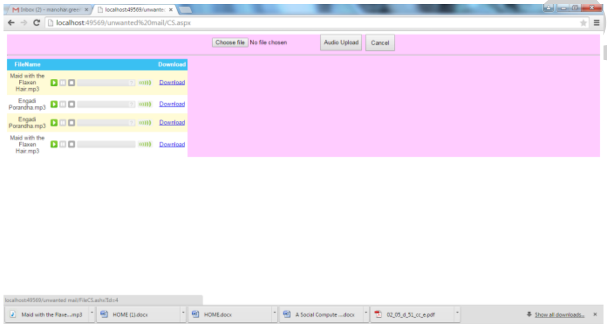


localhost:49569/unwanted%20mail/CS.aspx

Choose file No file chosen

FileName	Download
Maid with the Flaxen Hair.mp3	Download
Engadi Porandha.mp3	Download
Engadi Porandha.mp3	Download
Maid with the Flaxen Hair.mp3	Download

HOME (1).docx | HOME.docx | A Social Compute ...docx | 02_05_d_51_cc_e.pdf | thuraisingham12paisi.pdf



localhost:49569/unwanted%20mail/CS.aspx

Choose file No file chosen

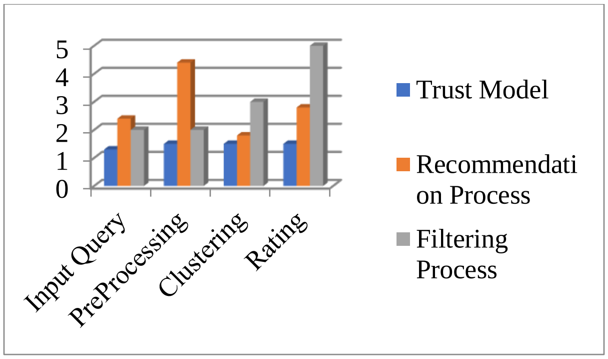
FileName	Download
Maid with the Flaxen Hair.mp3	Download
Engadi Porandha.mp3	Download
Engadi Porandha.mp3	Download
Maid with the Flaxen Hair.mp3	Download

localhost:49569/unwanted mail/FileCS.ashx?Id=4

Maid with the Flaxe...mp3 | HOME (1).docx | HOME.docx | A Social Compute ...docx | 02_05_d_51_cc_e.pdf

IMPLEMENTATION

A server is a computer program or a device that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model, and a single overall computation is distributed across multiple processes or devices. Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers. A client process may run on the same device or may connect over a network to a server on a different device.



CONCLUSION

To address two issues in this paper: (a) how exactly third party users launch an inference attack to predict sensitive information of users, and (b) are there effective strategies to protect against such an attack to achieve a desired privacy utility tradeoff. For the first issue, we show that collectively utilizing both attribute and link information can significantly increase prediction accuracy for sensitive information. For the second issue, we explore the dependence relationships for utility/public attributes, and privacy/public attributes. Based on these results, we propose a Collective Method that take advantages of various data manipulating methods to guarantee sanitizing user data does not incur a bad impact on data utility. Using Collective Method, we are able to effectively sanitize social network data prior to release. The solutions for the two addressed issues are proven to be effective towards three real social datasets.

REFERENCE

[1] https://www.researchgate.net/.

[2] http://www.imdb.com/.

[3] “Facebook beacon,” 2007.

[4] K. Heussner, “’gaydar’ on facebook: Can your friends reveal sexual orientation?” ABC News., 2009.

[5] C. Johnson, “Gaydar,” The Boston Blobe., 2009.

[6] http://www.pewinternet.org/2013/05/21/teens-social-mediaand- privacy/

[7] S. Nilizadeh, A. Kapadia, and Y.-Y.Ahn, "Community-enhanced de-anonymization of online social networks," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '14. New York, NY, USA: ACM, 2014, pp. 537– 548.

[8] A. Narayanan and V. Shmatikov, "De-anonymizing social networks," in Proceedings of the 2009 30th IEEE Symposium on Security and Privacy, ser. SP '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 173–187.

[9] L. Backstrom, C. Dwork, and J. Kleinberg, "Wherefore art thou r3579x?:Anonymized social networks, hidden patterns, and structural steganography," in Proceedings of the 16th International Conference on World Wide Web, ser. WWW '07. New York, NY, USA: ACM, 2007, pp. 181–190.

[10] B. Zhou, J. Pei, and W. Luk, "A brief survey on anonymization techniques for privacy preserving publishing of social network data," SIGKDD Explor.Newsl., vol. 10, no. 2, pp. 12–22, Dec. 2008.