Eleyon
SOUTH ASIAN JOURNAL OF
ENGINEERING AND TECHNOLOGY

Full Length Article

AN EFFICIENT PRIVACY MANAGEMENT SYSTEM INONLINE SOCIAL NETWORKS

T.Sureshkumar [a], K.Ganesh[b], K.Manikandan[b], S.Suryprakash [b], V.Renugapriya[b]

[a]Assistant professor, Department of Information Technology, Nandha College of Technology, Erode 638052 ,Tamilnadu ,India.
[b]UG Scholar, Department of Information Technology, Nandha College of Technology, Erode- 638052, Tamilnadu, India.
[b]UG Scholar,Department of Information Technology, Nandha College of Technology, Erode- 638052, Tamilnadu, India.
[b]UG Scholar , Department of Information Technology, Nandha College of Technology, Erode- 638052, Tamilnadu, India.
[b]UG Scholar , Department of Information Technology, Nandha College of Technology, Erode- 638052, Tamilnadu, India.

***Corresponding Author**
sureshkumartt@gmail.com
(T.Sureshkumar)
Tel.: 7871177875

Received : 15-12-2018
Reviewed : 25-01-2018
Revised : 7-02-2018
Accepted : 02-3-2019

DOI:

ABSTRACT:Online social networks (OSNs) have experienced tremendous growth in recent years and become a defect portal for hundreds of millions of Internet users. These OSNs offer attractive means for digital social interactions and information sharing, but also raise a number of security and privacy issues. While OSNs allow users to restrict access to shared data, they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users on.Data Provenance has achieved by comparison of packet header.

Keywords:UCB(Upper Confidence Bound), Osn(Online Social Network)

1.Introduction

Novel Topic-Sensitive Influencer Mining (TSIM) framework in interest-based social media networks. TSIM aims to find topical influential users and images. The influence estimation is determined with a hyper graph learning approach. In the hyper graph, the vertices represent users and images, and the hyper edges are utilized to capture multitier relations including visual-textual content relations among images, and social links between users and images. Algorithm wise, TSIM first learns the topic distribution by leveraging user-contributed images, and then infers the influence strength under different topics for each node in the hyper graph. We pursue a systematic solution to facilitate collaborative management of shared data in OSNs. We begin by examining how the lack of Multi Party Access Control (MPAC) for data sharing in OSNs can undermine typical data sharing the protection of user data. Some patterns with respect to multiparty authorization in OSNs identified. Based on these sharing patterns, an the core features of are also MPAC model is formulated to capture multiparty authorization requirements that have not been accommodated so far by existing access control systems Our control and models for OSNs. Model also contains a multiparty policy specification scheme. Meanwhile, since conflicts are inevitable in multi-party authorization enforcement, a voting mechanism is further provided to deal with authorization and privacy conflicts in our model.

II. LITERATURE SURVEY

(i) Hypergraph Learning With Hyper edge Expansion

Many tasks require clustering in a graph where each edge represents a similarity relation. Often, it is a co-occurrence relation that involves more than two items, such as the co-citation and co-purchase relations. The co-occurrence relation can be represented by a hyperedge that connects two or more vertices in a hyper graph. But most clustering algorithms, such as k-means, or spectral clustering, are defined for graphs but not hypergraphs. Therefore, hyperedge relations are often transformed into another graph that is easier to handle. For classification and clustering tasks, the hyperedge are usually transformed into cliques of edges. This category of techniques includes clique expansion, star expansion. With a vertex expansion, evaluating the goodness of clustering is done on the induced graph. For example, in a hyperedge of k vertices, a cut that separates the hyperedge into 1 and k − 1 vertices would cut k − 1 pairwise edges, while a cut that splits the vertices in two equal halves would have k

2/4 cut edges. Thus the vertex expansion would prefer an unbalanced clustering. To mitigate the problem of unbalanced clustering, it is proposed in star expansion and NHC to use the cluster volume as a normalizer for balancing the cluster sizes. But such normalization cannot completely eliminate the problem. We present the following example of vertex embedding to explain why the problem still exists.

(ii) Learning a Hidden Hypergraph

We also introduce an interesting combinatorial object, which we call an independent covering family. Basically, an independent covering family of a hypergraph is a collection of independent sets that cover all non-edges. An interesting observation is that the set of negative queries of any algorithm that learns a hypergraph drawn from a class of hypergraphs that is closed under the operation of adding an edge is an independent covering family of that hypergraph. Note both the class of r-uniform hypergraphs and the class of (r, Δ)-uniform hypergraphs are closed under the operation of adding an edge. This implies that the query complexity of learning such a hypergraph is bounded below by the minimum size of its independent covering families. In the opposite direction, we give subroutines to find one arbitrary edge from a hypergraph. With the help of the subroutines, we show that if we can construct small-sized independent covering families for some class of hypergraphs, we are able to obtain an efficient learning algorithm for it. In this paper, we give a randomized construction of an independent covering family of size O(r2 2r m log n) for r-uniform hypergraphs with m edges. This yields a learning algorithm using a number of queries that is quadratic in m, which is further improved to give an algorithm using a number of queries that is linear in m.

(i) Image Retrieval Via Probabilistic Hypergraph Ranking

Hypergraph based transductive algorithm is proposed to the field of image retrieval. Based on the similarity matrix computed from various feature descriptors, we take each image as a 'centroid' vertex and form a hyperedge by a centroid and its k-nearest neighbors. To further exploit the correlation information among images, we propose a novel hypergraph model called the probabilistic hypergraph, which presents not only whether a vertex vi belongs to a hyperedge ej, but also the probability that vi ∈ ej . In this way, both the higher order grouping information and the local relationship between vertices within each hyperedge are described in our model. To improve the performance of content-based image retrieval, we adopt the hypergraph-based transductive learning algorithm proposed in to learn beneficial information from both labeled and unlabeled data for image ranking. After feedback images are provided by users or active learning techniques, the hypergraph ranking approach tends to assign the same label to vertices that share many incidental hyperedges, with the constraints that predicted labels of feedback images should be similar to their initial labels.

(iii) User Interest And Social Influence Based Emotion Prediction For Individuals

Emotions are playing significant roles in daily life, making emotion prediction important. To date, most of state-of-the art methods make emotion prediction for the masses which are invalid for individuals. In this paper, we propose a novel emotion prediction method for individuals based on user interest and social influence. To balance user interest and social influence, we further propose a simple yet efficient weight learning method in which the weights are obtained from users' behaviours. The problem of emotion prediction for individuals is not trivial. So far, there are fewer works on emotion prediction for individuals. Emotions have long been viewed as passions produced on their own interest. However, from social as-pact, has shown that how happy you're is influenced by your social links to people in social networks. More recently, Tang's work quantitatively studies how an individual's emotion is influenced by his friends in social network.

III. EXISTING SYSTEM

Cryptographic mechanism-based security Social media technology mainly uses cryptographic security techniques for groups with dynamic memberships The group is any community or any cluster which shows same properties. The social media problems of security, privacy and anti-piracy can be overcome through cryptographic techniques like authentication, encryption etc.Each tag is an explicit reference that links to a user's space. For the user data, current OSNs indirectly require for regulating protection of users to be system and policy administrators their data, where users can restrict data sharing to a specific trusted users. OSNs often use user relationship and between trusted and set of group membership to distinguish untrusted users. For example, in Facebook, users can allow friends, friends of friends (FOF), groups, or public to access their personal authorization and data, depending on privacy requirements.

IV. PROBLEM DEFINITION:

- multi-armed bandit problem
- detecting the conflicts among different users' privacy policies, and then generating an aggregated policy that can resolve the conflicts to the largest extent collaborative privacy management in OSNs
- aggregated policy may cause a privacy loss to some of the users

Detection Strategy

Classification: Classification means researchers first to build a model for a group of classes or concepts, then use the model to predict class labels for test data. For example, to classify whether an email is email spam, web page is web spam.

Prediction: Prediction focuses on the continuous-valued functions of models researchers created. For example, scientists use the prepared models to forecast the economic growth in the next year.Classification and prediction are a two-step process, which means, model construction and model applications. Model construction means scientists first need to introduce a set of predefined classes, which called training dataset. Training dataset consists of tuples for building a model, and each tuple or sample belongs to a predefined class. At the same time, researchers need to make the classification rules, classification models, decision trees, decision rules, or math formulae, etc. Model application means to classify those unseen objects: researchers need to use an independent test data set to estimate the accuracy of the model, then use the model to classify unknown class labels. The training dataset needs to use some features to make a further application. As former researchers' experience, most of the features are web page top domains, languages, some words (body and title), average word length, anchor words, visibility of content, repeating keywords, the most common keywords, n-gram likelihood and so on.Suppose to explore the influence of spam in one OSN to another; we do not aim to show how great performance of detection only around one dataset. So we chose 10% original data to do the training work so that it can maintain the maximum independence and testability of posts in one social network, at the same time, it is more intuitional and beneficial to show the influence of spam related with same topics in other social network to the spam detection in that social network.

V. PROPOSED SYSTEM:

A high threshold indicates that the user has a relatively low tendency to share the data with others, and only when the majority of the involved users or users that are highly trusted agree to post the data, the data can finally be posted. By tuning the threshold, the user can make a trade-off between data sharing and privacy preserving. A trust-based mechanism is proposed for collaborative privacy management in OSNs. The trust values between users are associated with users' privacy loss, and the proposed mechanism can encourage users to be more considerate of other users' privacy. Trust-based privacy management mechanism based on threshold which the user makes the final decision on data posting. A high threshold indicates that the user has a relatively low tendency to share the data with others, and only when the majority of the involved users or users that are highly trusted agree to post the data, the data can finally be posted. By tuning the threshold, the user can make a trade-off between data sharing and privacy preserving. A bandit approach is proposed to adjust the parameter of the trust-based mechanism. By applying the UCB policy, the user can make a rational trade-off between data sharing and privacy preserving.

VI. MODULES

(i) User Profile Creation

A user profile (user profile, or simply profile when used in-context) is a collection of personal data associated to a specific user. A profile refers therefore to the explicit digital representation of a person's identity. A user profile can also be considered as the computer representation of a user model. A user profile is a visual display of personal data associated with a specific user, or a customized desktop environment. A profile refers therefore to the explicit digital representation of a person's identity. A user profile can also be considered as the computer representation of a user model. A profile can be used to store the description of the characteristics of person. This information can be exploited by systems taking into account the persons' characteristics and preferences. The user personal data store in ONLINE social networks (OSNs) database that details contain informs like first name, last name, username, password, email Id, gender etc.

(ii) Post Wall Creation

The Website wallpost is the most social network is enabling with photo sharing activities. Protected albums allow users to set their albums with access protection. This is one of the beneficial features from wallpost that who fear with photo scams on photo sharing websites. Photo tagging the option makes the photo search easier after a long period of time. Here ruse can give the names or keywords for photos that related to the photo in better to recognize easily. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. In this module user can add their or interested photos in their wall. This wall posting contains the photo, photo description, tag information are given by the user that details are stored in the OSNs database.

(iii) Multiparty Policy Access Control (MPAC)

Two steps are performed to evaluate an access request over MPAC policies. The first step checks the access request against the policy specified by each controller and yields a decision for the controller. The access or element in a policy decides whether the policy is applicable to a request. If the user who sends the request belongs to the user set derived from the accessory of a policy, the policy is applicable and the evaluation process returns a response with the decision (either permit or deny) indicated by the effect element in the policy. In the second step, decisions from all controllers responding to the access request are aggregated to make a final decision for the access request. Since data controllers may generate different decisions (permit and deny) for an access request, conflicts may occur. To make an unambiguous decision for each access request, it is essential to adopt a systematic conflict resolution mechanism to resolve those conflicts during multiparty policy evaluation.

(iv) Topic Distribution Learning

We utilize the image vertices and homogeneous hyper edges in the hyper graph to learn the topic distribution. We propose to develop a hyper graph regularized topic model to fully leverage both content and context information of images to help learn the potential topics of interest. However, in real-world scenarios, user-contributed social media data is inevitably noisy and the textual information associated with images is usually sparse, which makes it difficult to use the hyper graph regularized topic model to learn topics of interest accurately. Therefore, we first select the informative images with rich tags to identify the latent topics. Then we obtain the topic distribution for all images via collaborative representation based similarity propagation.

(v) Influence Ranking

Topic Sensitive Influence Ranking via Affinity Propagation Based on the learned topic distribution and the constructed hypergraph, we perform a topical affinity propagation on the hypergraph with the heterogeneous hyperedges for measuring influence regarding topics for each user and image. The affinity propagation algorithm is originally employed for clustering data to identify a subset of exemplars, which are used to best account for all other data points by passing similarity messages between data points. Affinity propagation can be applied whenever there is a way to measure or pre-compute a numerical value for each pair of data points, which indicates how similar they are. In our scenario, users exert influence on each other through images, which is reflected in the indirect user behaviors of favorite or comment links.

Algorithm:

1: for t = 1 to K do

2: Choose arm $It = t$

3: Observe and record the reward rIt,t

4: $r \leftarrow rIt,t$

5: $n_{It} \leftarrow 1$

6: end for

7: for $t = K + 1$ to T do

8: for i = 1 to K do

9.←1/ni ∑ r 1(I=i)

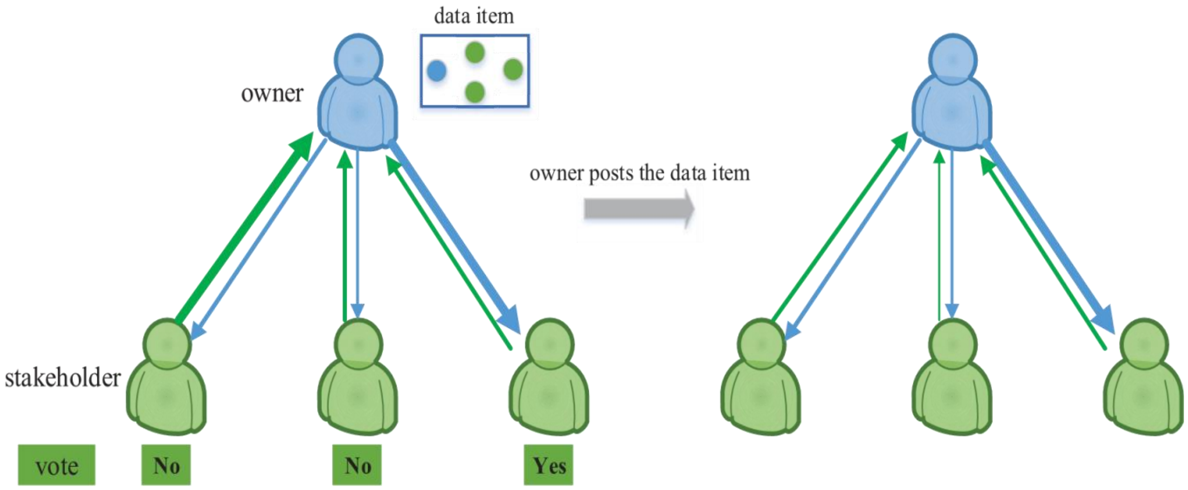
10: end for

12: Observe and record the reward $r_{It,t}$

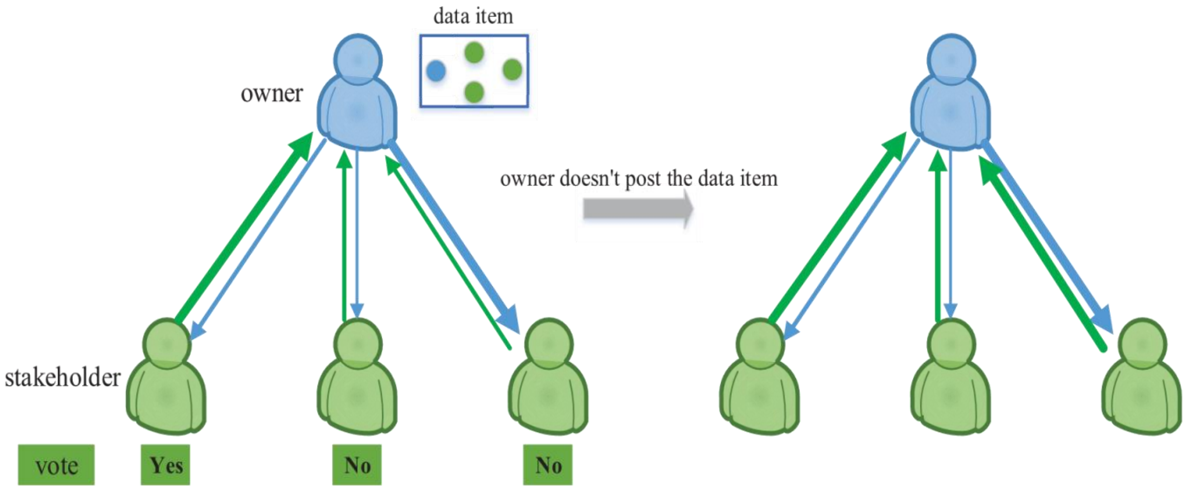
13: $r_t \leftarrow r_{It,t}$

14: $n_{It} \leftarrow n_{It} + 1$

15: end for



(a)



(b)

VII.CONCLUSION

That can make the privacy control for the individual user during the sharing process. And also user can be defined which user will be view and will not be view about their own data. Secure transaction and affinity propagation easily passible for using this set of algorithm. Data privacy can give businesses a competitive advantage. The general data production regulation

REFERENCES

1. H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in *Proc. 27th ACM Annu. Comput. Secure. Appl. Conf.*, Dec. 2011, pp. 103–112.
2. V.S. Sureshkumar "Optimized Multicloud Multitask Scheduler for Cloud Storage and Service by Genetic Algorithm and Rank Selection Method" ,International Journal of Advanced Science Engineering and Technology , pp:2-7, Issue 4, volume 3,2014
3. P. Auer, N. Cesa-Bianchi, and P. Fischer, "Finite-time analysis of the multigame bandit problem," *Mach. Learn.*, vol. 47, no. 2, pp. 235–256, 2002.
4. H. Hu, G.-J. Ahn, Z. Zhao, and D. Yang, "Game theoretic analysis of multiparty access control in online social networks," in *Proc. 19th ACM Symp. Access Control Models Technol.*, New York, NY, USA, Jun. 2014, pp. 93–102.

5. H. Hu, G. J. Ahn, and J. Jorgensen, “Multiparty access control for online social networks: Model and mechanisms,” *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 7, pp. 1614–1627, Jul. 2013.
6. V.S. Sureshkumar, A.Chandrasekar, “Fuzzy-GA Optimized Multi-Cloud Multi-Task Scheduler For Cloud Storage And Service Applications”, International Journal of Scientific & Engineering Research , Volume 4, Issue3, March-2013
7.