ISSN 2394-739X

IJRSET

International Journal for Research in Science Engineering and Technology

SECURE MULTIPARTY PRIVACY IN SOCIAL MEDIA WITH INDIVIDUAL ACCESS CONTROL

[1] Dr. P. Ponmuthuramalingam, [2] J. Jananipreetha,
[1] Associate Professor in Computer Science and Controller of Examinations,
[2] Research Scholar, PG & Research Department of Computer Science,
[1, 2] Government Arts College (Autonomous),
[1, 2] Coimbatore, INDIA.

ABSTRACT: In recent years, most popular websites are social media, it has largenetwork to connect a people and overload millions of internet user. These social networks offers to carry out desirable means for digital social inter connection and issue a various security and privacy problems. Right mechanism is provided to restrict shared data to minimize problem of multiuser shared data. A right approach is to carry out to allow the secure of shared data associated with multiple users in social network. . A proposed multiparty access control (MPAC) for data sharing in Online Social Network(OSN) can emasculate the security of user data has been proposed. Some typical data sharing patterns with respect to multiparty authorization in OSNs are also identified. Based on these data sharing patterns, an Multiparty Access control model (MPAC) is created to capture the core features of multiparty authorization requirements that have not been adapted so far by existing access control systems and models for OSNs. The proposed method implements a solution to privacy conflicts. Each organizer can set his privacy settings to the shared data item. It presents privacy conflicting sectors and helps in resolving the privacy conflicts and a decision is made whether or not to provide access to the shared data item. The proposed work uses C4.5 algorithm to classify the users and identify the trusted users to share with them.

Keywords: [Multiparty Access Control, privacy Conflicts, Social Networks, Facebook.]

1. INTRODUCTION

In the last era, the popularity of online social networks has exploded. Today, sites such as Facebook, MySpace, and Twitter combined reach over 500 million users daily. Users regularly upload personal stories, photos, videos, and lists of friends exposing private details to the public. To protect user data, privacy controls have become a central featureof social networking sites. More sophisticated applications of social network data includes tracking user behavior. However, one aspect of privacy remains largely unresolved. As photos, stories, and data are shared across the network, conflicting privacy obligation between friends can result in information being unintentionally exposed to the public, eroding personal privacy. While social networks allow users to control access to their own data, there is currently no mechanism to enforce privacy concerns over data uploaded by other users.Privacy preserving data mining is one of the most recent research areas of the data mining. Privacy preserving data mining allows sharing of the data between parties, but at the same time also conserves the privacy of the data. Privacy preserving data mining used to extracts the knowledge without divulging any information [7]. The purpose of secure multiparty computation is to give security and privacy. Facebook is a widespread social networking site with over thirty million users. Users can see the profiles of their friends and network. Profiles include pictures, dating preferences, birthdays, etc. Since the introduction of the Facebook Platform, profiles can also reveal third-party gadgets [5]. It provides a beginner's guide to help experts understand privacy rights related to the use of social networking sites and mechanism used to preserve privacy.

The main goal of this research work is to detect privacy conflicts and resolve using multiparty access control model mechanism. Using access control mechanism, users are able to share and tag images securely. This paper presents C4.5 algorithm to classify users to predict relationship between them. So that users can securely share and tag images with their friends. The main contribution is to secured share and tag images with access control. The organization of this work is given as follows: In section 2, an overview of the previous research works is given. In section 3, proposed methodology of this work is explained .In section 4, results are evaluated using java to prove the improvement of the proposed research work. In section 5, overall conclusion of this research work is explained.

2. RELATED WORKS

Besmer et al[5] described a Photo sharing and Tagging of photos on social network sites such as Facebook has caused users to lose control over their identity and information disclosures. The goal is to find privacy in sharing and tagging photos.

J.M. Such et al [7] introduces the problem of preserving privacy in computer applications and its relation to autonomous agents and Multi-agent Systems and identify some open challenges in the area of privacy and Multi-agent Systems. The author introduces the issue of privacy preservation and its relation to Multi-agent Systems. It plays a crucial role for preserving privacy.

Fogues et al [8] presents a list of privacy threats that can affect SNS users, and what requirements privacy mechanisms should accomplish to prevent these threats. Then, review current approaches and analyze to what extent they cover the requirements they have reviewed approaches that offer partial solutions to the most critical problems of privacy management on SNSs.

Wishart et al [9] presented a novel approach to collaborative policy authoring determined within the context of social networking. An approach permits the originators of content on the social network to specify policies for the content they upload.

Carminati et al [11] proposed a collaborative access control framework that enables multiple organizers of the shared item to collaboratively specify their privacy settings and to resolve the privacy conflicts among co-controllers with different requirements and desires. It enables multiple controllers of the shared item to collaboratively specify the privacy setting.

Hu et al [12] proposed a novel solution for privacy conflict detection and solution for collaborative data sharing in OSNs. This approach is used to enable collaborative privacy management of shared data in OSNs. It provides a systematic mechanism to identify and resolve privacy conflicts for collaborative data sharing.

3. PROPOSED WORK

In the Proposed System a Facebook application for the collaborative management of shared data have been implemented. To overcome the problem based on Online Social Networks, a systematic solution to facilitate collaborative management of shared data in OSN has been introduced. The user can share their data or images to their friends.

When the user tried to share other user's data, the request will be send to the owner of the data. After receiving the request, the owner of the data has rights to accept or reject the request. The User can only share other data after getting the approval form the data owner; otherwise the user cannot share the data to others. This work implements C4.5 algorithm to classify users according to privacy policy.

3.1 Multiparty access control (MPAC)

An MPAC model is devised to describe the main features of multiparty authorization requirements that have not been adapted so far by existing access control systems and models for OSNs.The system examine five scenarios—User Interface Design,profile sharing, relationship sharing, and content sharing, Image Tagging—to realize the hazards posted by the lack of collaborative control in OSNs. Facebook is taken as the running example in this discussion because it is currently the most widespread social network provider. In this approach, some privacy policies for social network users have been set. Through this mechanism users can protect their own shared images videos or content. Multiple parties in this network, before access the image of the original user, they wants to get access permission from the owner of the specific images. From both side some access controls in the network have been setted.

3.2 User Interface Design

This process is to provide a user interface, where the user can create their own account with needed information (username, password). Which is mainly created for provide a authentication for each individual user, who accessing the social media for some purpose. After authentication process users can select their multiple friends and add them. It provides functionalities to the user to register, login to the system, and update their information.

3.3 Profile sharing:

An attractive feature of some OSNs is to support social applications created by third-party creators to generate additional functionalities built on the top of users' profile for OSNs. To make matters more complex, social applications on current OSN policies can also consume the profile attributes of a users groups. In this situation, users can select certain pieces of profile attributes they are ready to share with the applications when their friends use the applications. At the same period, the users who are handling the applications may also want to control what information of their friends is accessible to the applications because it is feasible for the applications to suggest their private profile attributes through their friends' profile attributes. When an application accesses the profile characteristics of a user's friend, both the user and their friend want to acquire control over the profile attributes. Both the owner and the disseminator can specify access control policies to constrict the sharing of profile attributes.

3.4 Relationship sharing

An alternative characteristic of OSNs is that users can reveal their relationships with other members. Relationships carry potentially sensitive information that associated users may not want to expose. Most OSNs deliver mechanisms that users can control the display of their friend lists. A user can control only one direction of a relationship. In this scenario, authorization requirements from both the owner and the stakeholder would be deliberated. Otherwise, the stakeholder's privacy concern may be disrupted.

3.5 Content sharing

OSNs provides built-in mechanism whichallow users to connect and share contents with other members. OSN users can post status andcomments, upload photos and videos, tag their contents and share the contents with their friends. Users can also post contents to their friends. The shared contents may be connected with multiple users. All of them may denote access control policies to control over who can view this photo. All associated users should be allowed to describe access control policies for the shared content. OSNs also enable users to share others contents. All access control policies described by associated users should be enforced to regulate access of the content in disseminator's space. For a more complex case, the disseminated content may be further redisseminated by disseminator's friends, where efficient access control mechanisms should be applied in each procedure to regulate sharing behaviors the original access control policies should be continuously enforced to protect further dissemination of the content.

3.6 Image tagging

Image tagging is the important process used in the proposed system. The user can tag their thoughts or ideas through this media. After get authenticate login the user can access entire social media application like posting content, image or file sharing. This process also have a another privacy policy, that is if the user want to tag others tagged image or any other file they want to get approval from the owner of the tagged image. They want to send request for getting a permission. If the owner give a permission they can able to tag their image.

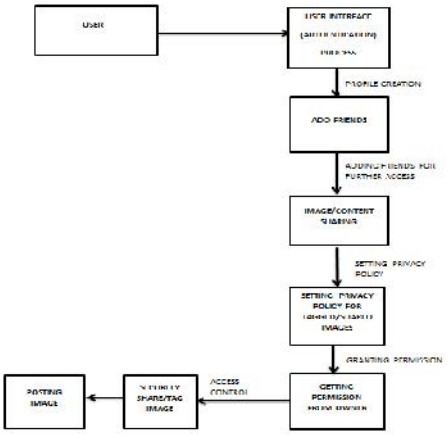
USER
USER INTERFACE (AUTHENTICATION) PROCESS
PROFILE CREATION
ADD FRIENDS
ADDING FRIENDS FOR FURTHER ACCESS
IMAGE/CONTENT SHARING
SETTING PRIVACY POLICY
SETTING PRIVACY POLICY FOR TAGGED/SHARED IMAGES
GRANTING PERMISSION
GETTING PERMISSION FROM OWNER
ACCESS CONTROL
SECURELY SHARE/TAG IMAGE
POSTING IMAGE

Figure 1- Flow diagram of Privacy Policy

3.7 C4.5 Algorithm

C4.5 algorithm is used for classify the users based on frequency. It is a decision tree based approach to classify the nodes into the several branches with sub branches. Step by step process were implemented to classify the social media users.

The following steps represent the whole process of C4.5 Algorithm

Step 1: Decision tree take number of nodes for processing (node1, node2,…..n).

Step 2: In next process, categorize the node based on decision making condition. Were the nodes are divided into sub nodes.

Step 3: Analyze the frequency between two nodes to add more nodes for further process.

Step 4: Calculate frequency between two individual node.

Freq (node1, node2) Step 5: After frequency calculation gain ratio will be predicted. Through this rationode request send to the adjacent node.

Through this algorithm process gain ratio will be calculated and node request send to adjacent node. After node request has been send, the user is the responsible for accept or reject a node request.

```
BuildTree($P_1$:$T_1$, C, A ;…; $P_n$:$T_n$ , C, A)
1) Compute the frequency freq($c_j$,T) foreach j∈[1, m]:
Foreach i∈[1, n],$P_i$ counts $T_i(c_j)=\{t|\ t.C=c_j\ , t\in T_i\ \}$;
$P_1$…,Pn jointly computefreq($c_{j,}$ T)$\sum_{i=1}^{n} |T_i(c_j)|/|T|$
2) Find freq($c_{jmax}$,T)=Max{ freq($c_j$ ,T)| j∈[1, m]};
3) If freq($c_{jmax}$,T)=1, or |T| is less then a certain value,
Create a leaf node L with the class$c_{jmax;}$
Compute the classification error of the node L;
Return L;
4) Create a decision tree node N;
5) Foreach attribute a∈A, $P_1$…,$P_n$ jointly compute information gain ratio GainRatio(a):
P1…,$P_n$ jointly determine a to be a discrete or continuous attribute;
If a is discrete and has l possible attribute values …,
P1,…,Pnjointly compute GainRatio(a) for the lsplittingn of T;
If a is continuous and has l attribute values v1,…,vl,
$P_1$…,Pnjointly compute GainRatio(a) for all the l-1 possible 2-splittings of T;
$P_1$…,Pn jointly find the 2-splitting with the
best GainRatio;
6) N.test=AttributeWithBestGainRatio;
7) ForeachT'=T1'∪…∪Tn' in the splitting of T
```

```
If T’ is Empty
Child of N is a leaf;$T_n$
Else
Child of N = BuildTree(P1: T1’, C, A-{a};…;Pn: Tn’, C, A-{a});
8) Compute the classification error of the node of N;
9) Return N;
```

```
In step 5 of the algorithm, GainRatio(a) is caculated as follows:
$Entropy\ (T) = \sum_{j=1}^{m} freq\ (c_{j,}T)\log_2 freq(c_{j,}T)$
$Entropy\ (T|a)=\sum_{k=1}^{i} \frac{|T(a=v_k)|}{|T|} Entropy(|T(a=v_k)|)$
Gain (a)=Entropy(T)-Entropy(T |a);
GainRatio(a)=Gain(a)/Split(a);
```

Algorithm 1: Pseudocode of the distributed C4.5 tree-construction algorithm

4. RESULT AND DISCUSSION

The work proposes novel methods for solving a friend recommendation in a privacy-preserving manner. In particular to the friend recommendation problem, the friendship between any two users can be treated as sensitive/private information. This compared the results that would have been obtained applying proposed mechanism and show the result how its accuracy increased compared with Linear and Naïve method.

Technique	No. of nodes (users)			
	25	50	100	150
Linear	86.2%	84.3%	81.4%	78.2%
NAÏVE	89.5%	87.1%	84.6%	81.2%
MPAC+C4.5	96.1%	94.5%	91.6%	90.0%

Table 1: Accuracy

Technique	No. of nodes(users)			
	25	50	100	150
Linear	4.7s	4.5s	4.2s	3.9s
NAÏVE	3.8s	3.4s	3.3s	3.1s
MPAC+C4.5	2.9s	2.7s	2.4s	2.2s

Table 2: Delay

Technique	No. of nodes(users)			
	25	50	100	150
Linear	85.3%	83.2%	81.6%	78.2%
NAÏVE	89.3%	84.5%	83.2%	81.3%
MPAC+C4.5	95.4%	94.2%	92.1%	79.5%

Table 3: Throughput

analysis of the proposed mechanism and algorithm with the Linear and Naïve method. Combining C4.5 algorithm and MPAC mechanism itprovide best result when compared to previous method. have been obtained applying proposed mechanism and show the result how its accuracy increased compared with Linear and Naïve method. their friend lists. Most often, when people In particular, compared the results that would by many on-line social networks (e.g., Facebook) where users are allowed to hide their friend lists. by many on-line social networks (e.g., Facebook) where users are allowed to hide Most often,

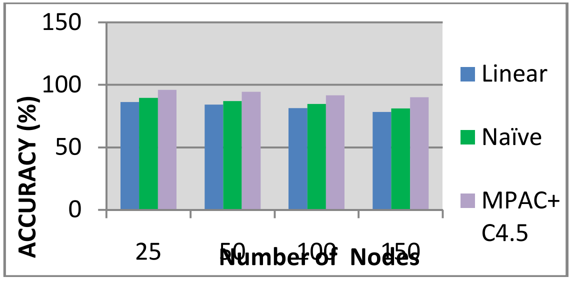

Figure 2- Accuracy

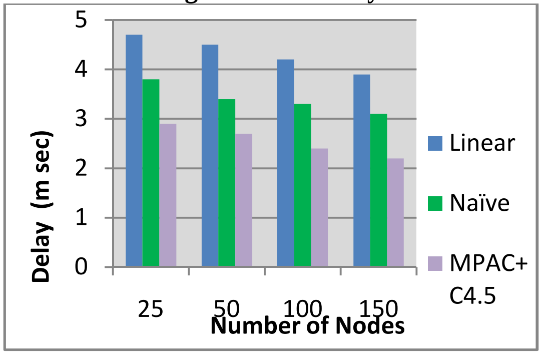

Figure 3: Delay

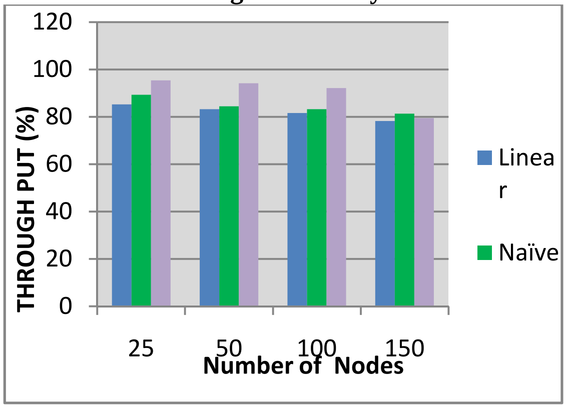

Figure 4: Throughput

CONCLUSION

Privacy plays a major important role in Social media. Multiparty access control model has been one of the best mechanisms used for privacy and security. A multiparty access control model for the shared data has been proposed. In this approach each of the controllers of the data item has the rights to set the privacy policy settings on the data item such that the controllers can specify who can view or cannot view the shared data item.. A solution for privacy conflict detection and resolution for collaborative data sharing in OSNs also have been implemented .This mechanism provides a flexible for detecting privacy conflicts. The conflict resolution mechanism considers privacy-sharing tradeoff by quantifying privacy risk and sharing loss. The proposed c4.5 algorithm has better results than the previous algorithms on the basis of accuracy and throughput.

REFERENCES

[1] Internet.org, “A focus on efficiency,” http://internet.org/efficiencypaper, Retr. 09/2014.

[2] K. Thomas, C. Grier, and D. M. Nicol, “unfriendly: Multi-party privacy risks in social networks,” in Privacy Enhancing Technologies. Springer, 2010, pp. 236–252.

[3] A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen, “We’re in it together: interpersonal management of disclosure in social network services,” in Proc. CHI. ACM, 2011, pp. 3217– 3226.

[4] P.Wisniewski, H. Lipford, and D.Wilson, “Fighting for my space: Coping mechanisms for sns boundary regulation,” in Proc. CHI. ACM, 2012, pp. 609–618.

[5] A. Besmer and H. Richter Lipford, “Moving beyond untagging: photo privacy in a tagged world,” in ACM CHI, 2010, pp. 1563– 1572.

[6] Facebook NewsRoom, “One billion- key metrics,” http://newsroom.fb.com/download-media/4227, Retr. 26/06/2013.

[7] J. M. Such, A. Espinosa, and A. Garc´ıa-Fornes, “A survey of privacy in multi-agent systems,” The Knowledge Engineering Review, vol. 29, no. 03, pp. 314–344, 2014.

[8] R. L. Fogues, J. M. Such, A. Espinosa, and A. Garcia-Fornes, “Open challenges in relationship-based privacy mechanisms for social network services,” International Journal of Human-Computer Interaction, no. In press, 2015.

[9] R. Wishart, D. Corapi, S. Marinovic, and M. Sloman, “Collaborative privacy policy authoring in a social networking context,” in POLICY. IEEE, 2010, pp. 1–8.

[10] A. Squicciarini, M. Shehab, and F. Paci, “Collective privacy management in social networks,” in WWW. ACM, 2009, pp. 521–530.

[11] B. Carminati and E. Ferrari, “Collaborative access control in online social networks,” in IEEE CollaborateCom, 2011, pp. 231–240.

[12] H. Hu, G.-J.Ahn, and J. Jorgensen, “Detecting and resolving privacy conflicts for collaborative data sharing in online social networks,” in Proc. ACSAC. ACM,2011, pp. 103–112. [Online]. Available: http://doi.acm.org/10.1145/2076732.2076747