Online Social Networks using User to User Relationship on Hierarchical Clustering

M.Divya Bharathi[1], M.Anand[2]

[1] Pg scholar, Department of Computer Science and Engineering, Sri Vidya college of Engineering & Technology ,Tamilnadu , India
[2]Assosiate Professor, Department of Information Technology, Sri Vidya college of Engineering & Technology, Tamilnadu, India

ABSTRACT

Online social networks have gained considerable popularity due to convenient and easy communication, social relationship with individuals with the same characteristics, anonymity, and no need to physical move. Discover potential malicious activity using collaborative control. In this paper, we propose a partitioning algorithm for providing the security for the user personal information for providing policy and privacy for multiple user to specify there authorization.

Keyword: - *Social network, security models, Tag analysis, network analysis.*

1. INTRODUCTION

Web mining is the use of data mining techniques to automatically discover and extract information from web documents and services. The information gathered by using the web mining and is evaluated by using traditional data mining techniques such as clustering and classification. Now a day's online social networks are used by the number of users and can share the lot of personal information through the social networks. In social networks for example Facebook , Linked In ect,. Users they can share their personal information, current social networks provide the security for the user's personal information but the user's data will be hacked by the third party user. To overcome this problem, the clustering concept will be used. In this paper we aim to explore a hidden structure of tagging practices and to build impact social network that consists of people and their using resources. Most of current OSNs implement very basic access control systems, by simply making a user able to decide which personal information is accessible by their direct contacts. In order to give more flexibility, some online social networks enforce variants of these settings, but the principle is the same. Users able to decide which personal information are accessible by the other members by marking a given item as public, private or accessible by their direct contracts. Online Social Networks are platforms those themselves and to connect to other members of the network through links .Recently, the popularity of OSNs is increasing significantly. Yuan cheng [13] propose common characteristic found in the most of this commercial and academic solution is that they mainly focus on user to user (U2U) relationship between accessing user and the resource owner, and at least implicitly assume ownership the only manifestation of user to resource (U2R) relationships. Since multiple users can express access control policies for a user or a resource, it is expected that there will be several policies applicable to the same access request from which will inevitably raise conflicts [13]. Providing functionality that allow online social networks [4] users to manage in a secure and private way the publication of their information and resources is a relevant and from trivial topic that has been under scrutiny from various research communities. Enforcement of access policies is access guaranteed by means of novel cryptographic primitive, Distance-Based Revocable Attribute Encryption (DBRA) for which we give an efficient implementation based on the Hidden Vector Encryption of [1] and the Hierarchical Identity-Based Encryption [2]. Relationship Based access-control policies are expressed by using the fragment of hybrid logic [5].

Hybrid logic removes an exponential penalty in existing attempts of specifying complex relationship such as at least three friends. Policy languages for relationship-based access control should be: not so expressive as to make reasoning intractable, based on robust mathematical foundation. Many existing Social Network systems (SNS) offer access control mechanisms that are at best rudimentary, typically permitting coarse-grained, binary visibility

control [19].Access control policy is typically defined in terms of attributes, but in many applications it is more natural to define permission in terms of relationship. Access control is specified and enforced in terms of attributes: authenticated properties that the resource, its system or context must possess in order to grant an access request.

2. PROPOSED METHOD

Online social network the users login to the social media and the user content will be send to the publishing, aggregating, integrating, and republishing the user content. Once all the process is completed the user content will be send to clustering. In this clustering process the user content will be clustered after that user uploaded image send to the user at that time the clustering concept is used. K-partitioning algorithm is used to set the clusters that is private, public and then uploaded image send it to the another user. User personal information will be secured. Each and every uploaded image will be send by the clustering algorithm, after the clustering the users data stored in the cluster database. Publishing which means that user's image and status will be uploaded. Aggregating means adding and sharing users content which aggregating the entire user content, aggregated used content send to the cluster database. Integrating include the request and response to the user. Republishing, all the published user data will be republished in this section.

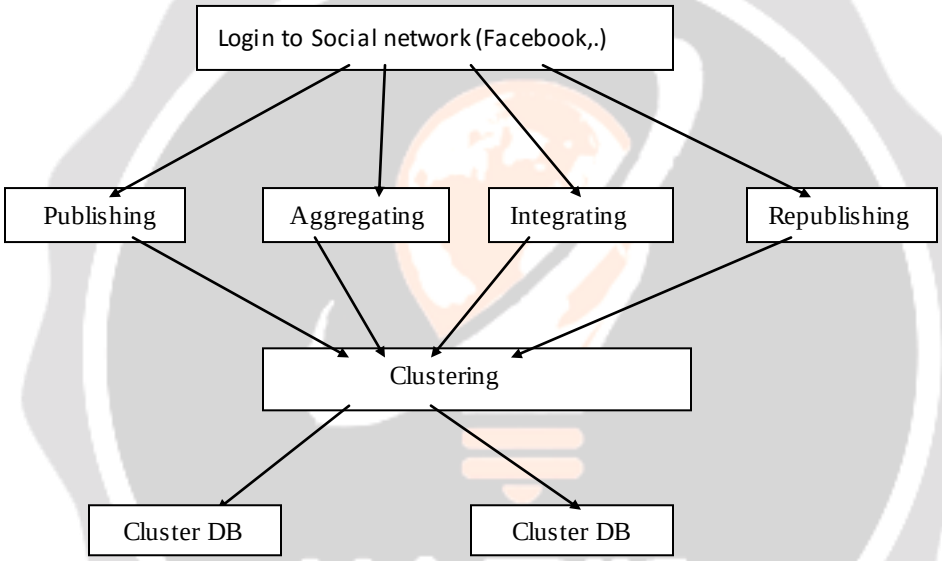

Fig 1: Block Diagram for proposed System

Republished users data will be stored in the cluster database. The tagging is the most popular social networking features. Tagging a user not only facilitates users to organize their photos, but also users to share and disseminate photos in OSNs. User can share their contents with other in their social network; otherwise, user can share other users content. Sharing other users, content OSNs encourage users to share others contents. While, OSNs users, can share their contents with other users, they can request other users, they can request other users to share their contents. When users share other users, they can request other to share their contents user shares other users content, it will be in turn posted in her/his profile. An accessing user carries access control polices and user to user relationships with other users. One of the most important issues in social networks is the security and privacy of users shared information. The large amount of personal information need appropriate security setting to be protected from unauthorized access and unwanted disclosure. An evaluation was done against several criteria drawn from these models for accessing them. For example, only Alice' directs friends can access her blogs, or only user who owns the photo or tagged users can modify the caption of the photo. For this purpose, we use social network analysis that reveals the structure of social relationship in a group or a community between the people. OSN users are exposed to potential threats to security and privacy of their data. Security and privacy incidents in OSNs have increasingly gained attention from both media and research community. Individual users and OSN provider should

be enabled to specify which access can be granted in terms of existing relationship. The users in community have slightly differentiated interests, and this makes several clusters from tagging activities.

3. RELATED WORK

Cluster analysis divides data into groups (cluster) that are meaningful, useful or both. If meaningful groups are the goal, then the clusters should capture the natural structure of the data. Classification of clustering include the exclusive clustering, overlapping clustering, hierarchal clustering, Fuzzy c-means clustering, and K-means clustering. Now focusing only the K-means clustering, because this algorithm is mainly used for partitioning. The user upload image to their friend at that time the K-means clustering concept is used. Now days any social network cannot build with the clustering concept. The K-means algorithm to cluster n objects based on attributes into k partitions, where k<n. To find the centers of natural clusters in the data. An algorithm for partitioning N data points into k disjoint subsets containing data points so as to minimize the sum of squares criterion. Classifying objects based on attributes, features into K number of group, K is positive integer number. The grouping is done by minimizing the sum of squares of distance between data and the corresponding cluster centroid. In existing system they can use the DFS, BFS path checking algorithm. One the major drawback of this algorithm is OSN systems enforces a simple and limited relationship-based access control mechanism. Regulates the access information with relationship depth, and trust value. Specifically, each trust value assigned to a person is static and subjective. The existing research in OSNs covers the issue of computing individual recommendations. Relationship between the accessor and the target/controlling user must satisfy the graph rules specified in access control policies regarding the given request. The path checking algorithm take as input the social graph G, the path pattern path and hopcount limit *hopcount* specified by *path spec* in the policy, the starting node s specified by start and the evaluating node t which is the other user involved. User-specified polices specify how individual users want their resources or services related to them to be released to other users in the system. Policies are specific to actions against a particular resources or user. the social graph is modeled as a simple graph. Further we only allow simple path with no repeating nodes. Avoiding repeating nodes on the relationship path prevents unnecessary iterations among nodes that have been visited already and unnecessary hops on these repeating segments. System- specified policies allow the system to specify access control on user and resources. Different from user policies, the statements in system policies are not specific to particular accessing user or target, but rather focus on the entire set of users or resources types. The existing model in this paper only permit the specification of paths, the model can be extended to capture this type of policies by utilizing attribute information of users and relationships. The disadvantages of existing model are they share images that they do not allow different relationship types and multiple possible types on each hop. In this paper, we proposed a user to user relationship-based access control model, allowing users the ability to express more sophisticated and fine-grained access control policies in terms of type pattern and depth of relationships among users in the network. Most existing OSN systems enforce a rudimentary and limited relationship-based access control mechanism, offering users the ability to choose from a predefined policy vocabulary, such as “public”, ”private”, ”friend” or “friend of friend”. Google+ and Facebook introduce customized relationship, namely “circle” and “friend list”, providing users richer options to differentiate distinctly privileged user groups. OSNs are becoming the most prevalent manifestation of user-generated content platforms.

4. ALGORITHM

The cluster centroid is middle of a cluster. A Centroid is a vector containing one number for each variable, where each number is the mean of a variable for the observations in that cluster. Cluster location is measured by centroid. There are K clusters are used, always at least one item in each cluster. The clusters are non-hierarchical and they do not overlap, with a large number of variables, k-means may be computationally faster than hierarchal cluster (if k is small). The use of this algorithm is to group the user into any cluster. To make partition the shared data to each cluster.

K- Partitioning Algorithm

In this proposed system use the K-partitioning algorithm. This algorithm mainly used for the partitioning. Groups of users identified by using this algorithm.

1. Start

2. {

3. Take k samples from total of N randomly as the as the centriod of each cluster.

4 Now calculate the D of the remaining N- k samples to each centroid and assign them to the cluster with the nearest centroid.

5.}

6. After each assignment, again calculate the centroid of the attainment cluster.

7. Now go to step 2 until find no new assignment.

8. Stop.

The proposed algorithm use the cluster concept it easy to the user and share their personal information. Given a k, find a partitioning criterion 1. Global optimal: exhaustively enumerate all partitions. 2. Heuristic methods: K-means and K- modules algorithms. 3. K-means: Each cluster is represented by the center of the cluster. 4. K-medoids or PAM (Partition around medoids): Each cluster is represented by one of the objects in the cluster. Strengths of this algorithm is relatively efficient: O (tkn), where n is # iterations. Normally, k, t<<n. Often terminates at a local optimum. The global optimum may be found using techniques such as simulated annealing and generic algorithms. The clustering algorithm used for grouping the user and their friends. It provide the security for the user and resources person. The overall clustering method is controlled by the admin. Admin is responsible for the user data's and remaining resources used in the OSN. The surveillance cluster maintains only the user's personal information. This algorithm provides the efficiency and accesses of resources.

5. PERFORMANCE ANALYSIS

The Facebook server provides an entry point via the Facebook application page, and provides references to photos, friendships, and feed data through API calls. Facebook server accepts inputs from users, and then forwards them to the application server. The application server is responsible for the input processing and collaborative management of shared data. Fig 2 and 3 represent the group size and latency of users shared information and location and search performance of each user in the social network.

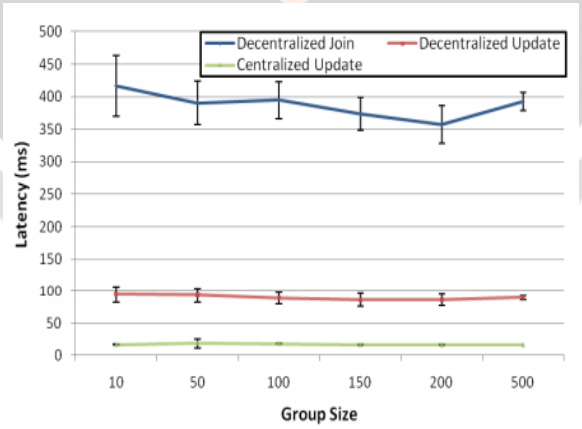

Chart 1: Joint and Update Performance

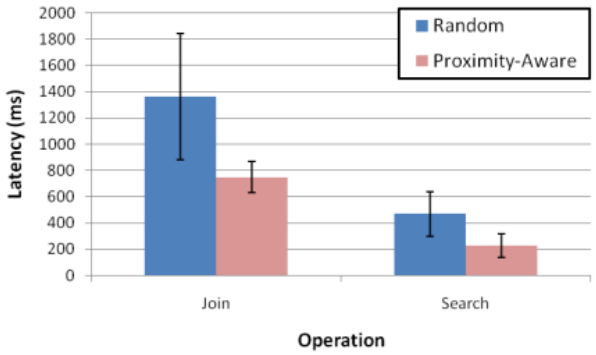

Chart 2: Location and search performance

When access requests are made to the decision-making portion in the application server results are returned in the form of access to photos or proper information about access to photos. In addition, when privacy change impact information to the interface to alert the user. Using the JavaScript and PHP SDK, it accesses users' Facebook data through the graph API and Facebook query language. Once a user installs in her/his Facebook space and accepts the necessary permissions, can access a user's basic information and contents. Especially, can retrieve and list all photos, which are owned or uploaded by the user, or where the user was tagged. Once information is imported, the user accesses through its application page on Facebook, where she/he can query access information, set privacy for photos that she/he is a controller, or view photos she/he is allowed to access. A core component of is the decision-making module, which processes access requests and returns responses (either permit or deny) for the requests.

6. CONCLUSION

In this paper, we propose User to User Relationship based on the hierarchical clustering model based on the clustering. User can categorize people based on attributes and maintains privacy of his own account. Along with categories users are able to communicate by encryption data to make the communication more secure. Category based sharing is nothing attribute based sharing were user can control whom to give access for which type of data. This is new area of data communication that fulfills some security issue. We were able to identify how the surveillance and social privacy researches ask complementary question. We leave as a topic of future research a more thorough comparative analysis of all approaches. We believe that such reflection may help us better address the privacy problem we experience as OSN users, regardless of whether we do so as activists or consumers.

7. REFERENCES

[1] S. Braghin, V.Iovino, G. Persiano, and A.Trmbetta, Secure and policy-private resource sharing in an online social work. In PASSAT 2011, pages 872-875. IEEE, 2011.

[2] B. Carminati and E. Ferrari. Collaborative access control in online social networks. In collaborate Com 2011, pages 231-240. IEEE, 2011.

[3]. B. Carminati, E. Ferrari, and J. Giardi Performance analysis of relationship-based control in osns. In IEEE IRI 2012, pages 449-456, 2012.

[4]. G. Bruns, P. W. Fong, I. Siahaan, and M. Huth. Relationship-based access control: its expression and enforcement through hybrid logic. In Proceedings of the second CODASPY, pages117–124. ACM, 2012**.**

[5]. B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B.Thuraisingham. Semantic web-based social network access control. Computers and Security, 30(2C3), 2011.

[6]. Y.chengg, J. Park, and R. Sandhu. Relationship-based access control for online social networks: Beyond user-to-user relationships. In PASSAT 2012, pages 646–655. IEEE, 2012.

[7]. B.Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, pages 1734–1744.Springer, 2006.

[8]. B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. A semantic web based framework for social network access control. In Proceedings of the 14th ACMSACMAT, pages 177–186. ACM, 2009

[9]. B. Carminati, E. Ferrari, and A. Perego. A decentralized security framework for web-based social networks. Int. Journal of Info. Security and Privacy, 2(4), 2008.

[10]. C. Gates. Access control requirements for Web 2.0 security and privacy. IEEE Web 2.0, 2007.

[11]. M. Hart, R. Johnson, and A. Stent. More content-less control: Access control in the Web 2.0. IEEE Web 2.0, 2007.

[12]. H. Hu and G.-J. Ahn. Multiparty authorization framework for data sharing in online social networks. In Data and Applications Security and Privacy XXV, pages 29–43. Springer, 2011.

[13].H. Hu, G.-J. Ahn, and J. Jorgensen. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In Proceedings of the 27th ACSAC, pages 103–112. ACM, 2011.

[14].J. Park, R. Sandhu, and Y. Cheng. ACON: Activity-centric access control for social computing. In ARES 2011, pages 242–247. IEEE, 2011.

[15].J. Park, R. Sandhu, and Y. Cheng. A user-activity-centric framework for access control in online social networks. Internet Computing, IEEE, 15(5):62–65, 2011.