Eleyon

SOUTH ASIAN JOURNAL OF ENGINEERING AND TECHNOLOGY

Full Length Article

Trust Based Allocating And Sharing Resources Via Social Networks With Multiparty Secured Access Control

D.Kavin kumar[a], A.Kavipriya[a] J.Logeshwaran[a], E.Nandhakumar[a], M.Umamaheswari[b]

[a] *Student,Department of CSE, K.S.R College of Engineering, Tiruchengode, Tamilnadu, India*

[b] *Assistant Professor,Department of CSE, K.S.R College of Engineering, Tiruchengode, Tamilnadu, India*

***Corresponding Author**
M.Umamaheswari

ABSTRACT: Online social networks (OSNs) have experienced tremendous growth in recent years. 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. This paper enhances existing and introduces new social network privacy management models and measures their human effects. First, it introduces a mechanism using proven clustering techniques that assists users in grouping their friends for traditional group-based policy management approaches. It found measurable agreement between clusters and user-defined relationship groups. Second, it introduces a new privacy management model that leverages users' memory and opinion of their friends (called example friends) to set policies for other similar friends. Finally, it explores different techniques that aid users in selecting example friends. It is found that by associating policy temples with example friends (versus group labels), users author policies more efficiently and have improved perceptions over traditional group-based policy management approaches. In addition, the results show that privacy management models can be further enhanced by utilizing user privacy sentiment for mass customization. By detecting user privacy sentiment (i.e., an unconcerned user, a pragmatist or a fundamentalist), privacy management models can be automatically tailored specific to the privacy sentiment and needs of the user.

Keywords: Friend book, Privacy Policy Inferences, Trust Base Social Network, Filter Content

1 Introduction

The papers leverages traditional group-based policy management as our baseline and progressively improve upon this privacy management model. With each new enhancement, we measure their human effects including cluster/user defined relationship group alignment, user privacy sentiment, efficiencies and user perceptions. The thesis introduces a user-assisted friend grouping mechanism that enhances traditional group-based policy management approaches. Assisted Friend Grouping leverages proven clustering techniques to aid users in grouping their friends more effectively and efficiently.

It introduces a new privacy management model that is an improvement over traditional group-based Policy management approaches. The new paradigm leverages a user's memory and opinion of their friends to set policies for other similar friends, which we refer to as Same-As Policy Management. Users associate the policy with an example friend and in doing so have this friend in the forefront of their mind. This allows users to be more selective and careful in assigning permissions. Users are thinking of people, not groups. Using a visual policy editor that takes advantage of friend recognition and minimal task interruptions, same-As Policy Management demonstrated improved performance and user perceptions over traditional group-based policy management approaches. It further enhances Same-As Policy Management by introducing Example Friend Selection—two techniques for aiding users in selecting their example friends that are used in developing policy templates. Both techniques reduced policy authoring times and were positively perceived by users. In addition, the thesis proposes an approach to enable the protection of shared data associated with multiple users in OSNs.

2. Related Works

Barbara Carminati stated that the existence of online social networks that include person specific information creates interesting opportunities for various applications ranging from marketing to community organization. On the other hand, security and privacy concerns need to be addressed for creating such applications. Improving social network access control systems appears as the first step toward addressing the existing security and privacy concerns related to online social networks. To address some of the current limitations, they have created an experimental social network using synthetic data which they then used to test the efficacy of the semantic reasoning based approaches they have previously suggested.

YUAN CHENG stated that users and resources in online social networks (OSNs) are interconnected via various types of relationships. In particular, user-to-user relationships form the basis of the OSN structure, and play a significant role in specifying and enforcing access control. Individual users and the OSN provider should be allowed to specify which access can be granted in terms of existing relationships.

They proposed a novel user-to-user relationship-based access control (UURAC) model for OSN systems that utilizes regular expression notation for such policy specification. They developed a path checking algorithm to determine whether the required relationship path between users for a given access request exists, and provide proofs of correctness and complexity analysis for this algorithm.

PAUL DUNPHY stated that Graphical password systems based on the recognition of photographs are candidates to alleviate current over-reliance on alphanumeric passwords and PINs. However, despite being based on a simple concept – and user evaluations consistently reporting impressive memory retention – only one commercial example exists and overall take-up is low. Barriers to uptake include a perceived vulnerability to observation attacks; issues regarding deployability; and the impact of innocuous design decisions on security not being formalized.

CATHERINE DWYER stated that it is not well understood how privacy concern and trust influence social interactions within social networking sites. An online survey of two popular social networking sites, Facebook and MySpace, compared perceptions of trust and privacy concern, along with willingness to share information and develop new relationships. Members of both sites reported similar levels of privacy concern. Facebook members expressed significantly greater trust in both Facebook and its members, and were more willing to share identifying information. Even so, MySpace members reported significantly more experience using the site to meet new people. These results suggest that in online interaction, trust is not as necessary in the building of new relationships as it is in face to face encounters. They also show that in an online site, the existence of trust and the willingness to share information do not automatically translate into new social interaction. This study demonstrated online relationships can develop in sites where perceived trust and privacy safeguards are weak.

LUJUN FANG stated that Privacy is an enormous problem in online social networking sites. While sites such as Facebook allow users fine-grained control over who can see their profiles, it is difficult for average users to specify this kind of detailed policy. In this paper, they proposed a template for the design of a social networking privacy wizard. The intuition for the design comes from the observation that real users conceive their privacy preferences (which friends should be able to see which information) based on an implicit set of rules. Thus, with a limited amount of user input, it is usually possible to build a machine learning model that concisely describes a particular user's preferences, and then use this model to configure the user's privacy settings automatically.

3. Existing system

The existing system introduces three new improvements to privacy management models:

- Assisted Friend Grouping an incremental improvement to traditional group-based policy management.
- Same-As Policy Management a new paradigm improvement over traditional group-based policy management.

Online social networks (OSNs) have experienced tremendous growth in recent years. 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.

This paper enhances existing and introduces new social network privacy management models and measures their human effects. First, it introduces a mechanism using proven clustering techniques that assists users in grouping their friends for traditional group-based policy management approaches. It found measurable agreement between clusters and user-defined relationship groups. Second, it introduces a new privacy management model that leverages users' memory and opinion of their friends (called example friends) to set policies for other similar friends. Finally, it explores different techniques that aid users in selecting example friends. It is found that by associating policy temples with example friends (versus group labels), users author policies more efficiently and have improved perceptions over traditional group-based policy management approaches. In addition, the results show that privacy management models can be further enhanced by utilizing user privacy sentiment for mass customization. By detecting user privacy sentiment (i.e., an unconcerned user, a pragmatist or a fundamentalist), privacy management models can be automatically tailored specific to the privacy sentiment and needs of the user.

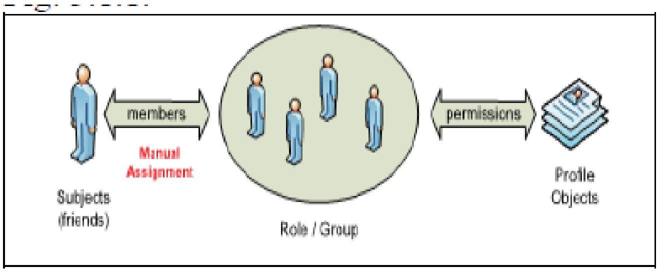


Fig 1.1 Social Group

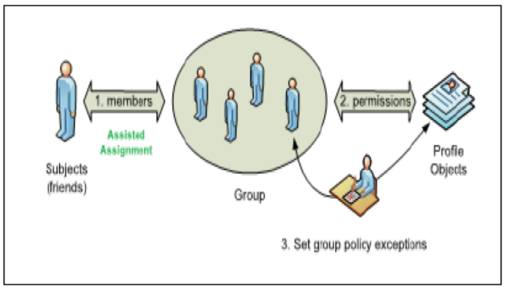


Fig 3.2 Privacy Group

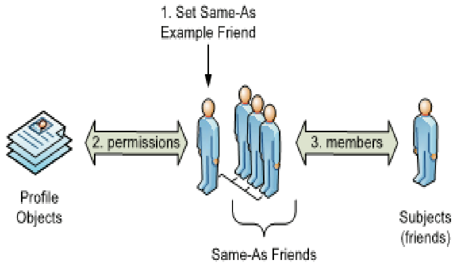
Within the proposed prototype, each friend is presented to the user in the center of a friend grouping page, refer to Fig. 3.1.3. The user is asked to select, for each friend, the group that best represents their relationship. They can either "drag" the friend to the appropriate relationship group on the page. Or the user can click the representative relationship group name.

To assist users in populating their relationship groups, we leverage the Clasuet Newman Moore (CNM) network clustering algorithm. This clustering algorithm analyzes and detects community structure in networks by optimizing their modularity. Modularity is a metric that describes the quality of a specific proposed division of a network into communities. This prototype clusters the user's social network graph creating CNM clusters (or groups) of friends.

During friend grouping, the new concept presents the friends to the user in CNM group order as recommendations. For example, Bob has 50 friends and clustering his social network graph using CNM produces five clusters. The new concept presents to Bob, as recommendations for grouping, all the friends of one CNM group before presenting the friends of each subsequent CNM group. The premise is that CNM groups roughly align with user-defined friend populated relationship groups.

B. Same-As Policy Management

In group-based policy management, the user must first group their friends. After which, they must select group permissions (setting the group policy). Finally, friend-level exceptions to the group policy are set. A user's attention (mental model) is focused in multiple areas. Whereas in Same-As Policy Management, the user's attention is focused on a specific friend. Users leverage their memory and opinion of a friend to set policies for other like friends. In essence, we use a friend recognition approach, with minimal task interruptions, to aid the user in setting policies.



PRIVACY SETTINGS ALGORITHM

INPUT: User U, Privacy Set {View, Share, Comment} PS, (Relationship Types) RT

OUTPUT: Privilege Assigned User UPS

```
UPS U
For each rt in RT
    Add rt to UPS.Relationship Types
    V = Get View Uploaded Content Status {Yes, No}
    UPS[rt].View V
    Rt.S = Get Share Uploaded Content Status {Yes, No}
    UPS[rt].Share S
    Rt.C = Get Comment Uploaded Content Status {Yes, No}
    UPS.[rt].Comment C
Next
return UPS
```

ASSISTED FRIEND SELECTION ALGORITHM
INPUT: User U, Requested User RU
OUTPUT: % Related to User U's Current Friends CF List

```
TU Find Total Users in CF of U

Sum = 0
For each rt in RTU
    UCrt = Find users count UC in CF already related (with U as rt) with RU
    Sum = Sum + UCrt
Next
Percentage = (Sum / TU) * 100
return Percentage
```

CLUSTER FORMATION ALGORITHM
INPUT: User List UL, Relation Types RT
OUTPUT: Relation Type Clusters RTC

```
RTC null
For each rt in RT
    RTC RTC rt
Next
For each U in UL
    Max =0
    RT =empty
    For each rt in RTU
        UC Total User Count in rt
        if UC > Max
            Max = UC
            RT = rt
        end if
    Next
    RTC[rt] RTC[rt] U
Next
return RTC
```

4. Experimental results

A. Worst Case Analysis

Table 5.1 shows the result of A3P and Enhanced Collaborative Tagging Model [ECTM]. The table contains tag percentage [TP], collaborative tag percentage [TP] and worst case error rate per user communication details shown.

S.NO	TP	A3P USERS (WC)	TP	Collaborative USERS (WC)
1	40	25.00	50	20.00
2	50	20.00	60	16.60
3	60	16.60	70	14.28
4	70	14.28	80	12.50
5	80	12.50	90	11.11

Table 5.1 Worst Case Analysis A3P AND ECTM

Fig 6.1 shows the result of existing and proposed Collaborative Tagging model. The figure contains tag percentage [TP], proposed tag percentage [TP] and worst case error rate per user communication details shown.

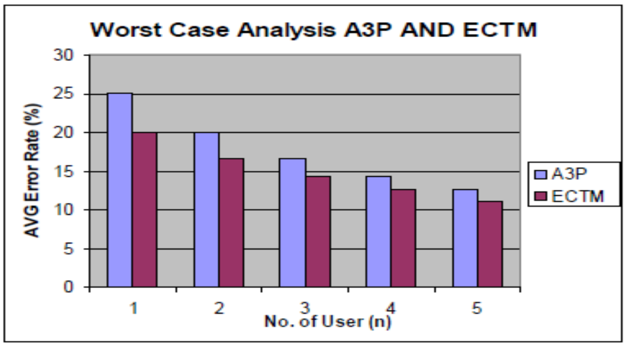
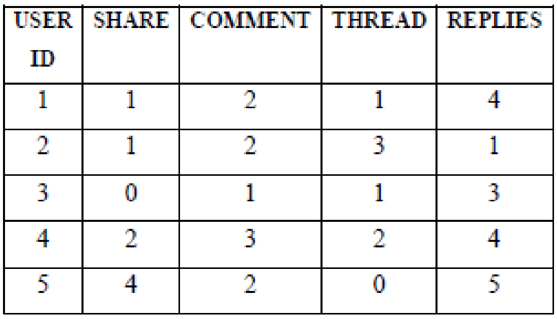


Fig 5.1 Worst Case Analysis A3P AND ECTM

B. User Wise Processed Result

Table 5.2 and Fig 5.2 is describing the experimental result for user wise process result in proposed system. The table contains user id, share id count, comment count details, thread count details, and replies details count are shown below.



USER ID	SHARE	COMMENT	THREAD	REPLIES
1	1	2	1	4
2	1	2	3	1
3	0	1	1	3
4	2	3	2	4
5	4	2	0	5

Access Count = (User Request * No. of. User)

Table: 5.2 User Wise Processed Result

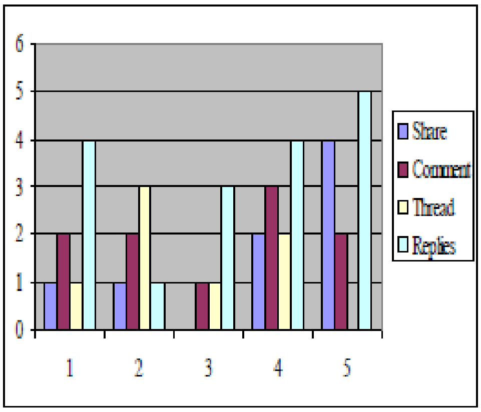


Fig 5.2 User Wise Processed Result

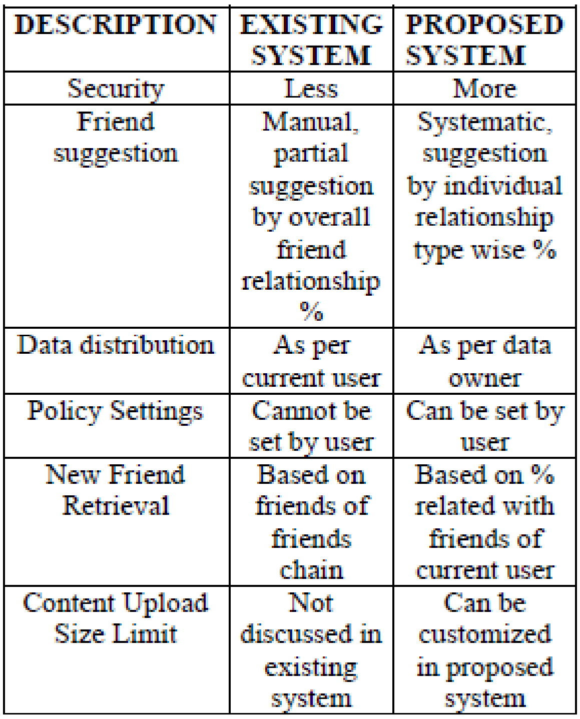
1. It is found that the friend is based on only friends of friends chain in existing system.

2. It is found that the friend suggestion not shows the percent related with friends group of the current user.

3. The proposed system shows the friends percent related with current users all relationship types.

4. All the top members of clusters (relationship types) can be retrieved in proposed system and first member having more percentage is filtered out.

5. Data is propagated to all users as per the policy settings provided by current user in existing system.



DESCRIPTION	EXISTING SYSTEM	PROPOSED SYSTEM
Security	Less	More
Friend suggestion	Manual, partial suggestion by overall friend relationship %	Systematic, suggestion by individual relationship type wise %
Data distribution	As per current user	As per data owner
Policy Settings	Cannot be set by user	Can be set by user
New Friend Retrieval	Based on friends of friends chain	Based on % related with friends of current user
Content Upload Size Limit	Not discussed in existing system	Can be customized in proposed system

6. Data is propagated to all users as per the policy settings provided by data owner in proposed system.

7. Content usage is more secure in proposed system since if the data owners prevent the data to be hidden to selected users, then the content will not be propagated to those users through any of the intermediate users.

8. Records such that total requests versus accepted records count for friend requests can be found out from proposed system

5.Conclusion

The system is very flexible and user-friendly, so the maintenance based on the changing environment and requirements can be incorporated easily. Any changes that are likely to cause failures are prevented with security and preventive measures could be taken. The coding is done in understandable and flexible method program which helps easy changing. The project has covered almost all the requirement. Further requirements and improvements can easily be done since the coding in mainly structured or modular in nature. Improvements can be appended by changing the existing modules or adding new modules. Several areas to be developed in future, so the application must be upgraded for the new ones required and it is possible to modifications according to new requirements and specifications.

Facilities like fast data backup and restoration in case of data loss situations.

✓ Facilitate users to process the authenticate and spam the unwanted comment in the transaction.

The application is designed such that the required enhancements can be integrated with each module easily with less integration work without modifying the present system.

References

[1] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds,” Proc. 16th ACM Conf. Computer and Comm. Security (CCS ’09), pp. 199-212, 2009.

[2] Y. Zhang, A. Juels, M.K.M. Reiter, and T. Ristenpart, “Cross-VM Side Channels and Their Use to Extract Private Keys,” Proc. ACM Conf. Computer and Comm. Security (CCS ’12), pp. 305-316, 2012.

[3] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, “All Your Clouds Are Belong to Us: Security Analysis of Cloud Management Interfaces,” Proc. Third ACM Workshop Cloud Computing Security Workshop (CCSW ’11), pp. 3-14, 2011.

[4] S. Bugiel, S. Nu ̈ rnberger, T. Po ̈ppelmann, A.-R. Sadeghi, and T.Schneider, “AmazonIA: When Elasticity Snaps Back,” Proc. 18th ACM Conf. Computer and Comm. Security (CCS ’11), pp. 389-400, 2011.

[5] G. Danezis and B. Livshits, “Towards Ensuring Client-Side Computational Integrity (Position Paper),” Proc. ACM Cloud Computing Security Workshop (CCSW ’11), pp. 125-130, 2011.

[6] S. Groß and A. Schill, “Towards User Centric Data Governance and Control in the Cloud,” Proc. IFIP WG 11.4 Int’l Conf.

[7] Open Problems in Network Security (iNetSeC), pp. 132-144, 2011.

[8] M. Burkhart,M. Strasser, D. Many, and X. Dimitropoulos, “SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics,” Proc. USENIX Security Symp., pp. 223-240, 2010.

[9] D. Hubbard and M. Sutton, “Top Threats to Cloud Computing V1.0,” Cloud Security Alliance, http://www. cloudsecurityalliance.org/topthreats, 2010.

[10] Amazon Elastic Compute Cloud (EC2).http://aws.amazon.com/ec2/

[11] Microsoft Azure Services Platform.http://www.microsoft.com/azure/default.mspx

[12] Rackspace Mosso. http://www.mosso.com/

[13] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Commun. ACM, 53(4):50–58, 2010.

[14] R. Meushaw and D. Simard. A network on a desktop. NSA Tech Trend Notes, 9(4), 2000. http://www.vmware.com/pdf/TechTrendNotes.pdf.

[15] P. England and J. Manferdelli. Virtual machines for enterprise desktop security. Information Security Technical Report, 11(4):193 – 202, 2006.

[16] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh. Terra: a virtual machine-based platform for trusted computing. In ACM Symposium on Operating Systems Principles, pages 193–206. ACM, 2003.

[17] O.Acii ̧cmez. Yet another microarchitectural attack: Exploiting I-cache. In ACM Workshop on Computer Security Architecture, pages 11–18, October 2007.

[18] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. In 16th ACM Conference on Computer and Communications Security, pages 199–212, 2009.

[19] Gnu Privacy Guard. www.gnupg.org, 2012.

[20] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer. Openpgp message format. Technical report, RFC 2440, November, 1998.

[21] McIntosh, M., and Austel, P. XML Signature Element Wrapping attacks and Countermeasures. In SWS '05: Proceedings of the 2005 workshop on Secure web services (New York, NY, USA, 2005), ACM Press, pp. 20-27.

[22] Nadalin, A., Kaler, C., Monzillo, R., and Hallam-Baker, P. Web Services Security: SOAP Message Security 1.1 (WS-Security 2004). OASIS Standard Specification (2006).

[23] McIntosh, M., and Austel, P. XML Signature Element Wrapping attacks and Countermeasures. In SWS '05: Proceedings of the 2005 workshop on Secure web services (New York, NY, USA, 2005), ACM Press, pp. 20-27.

[24] NIST. The NIST Definition of Cloud Computing (Draft). 2011. Special Publication 800-145 (Draft).