Detecting And Resolving Privacy Conflicts in Online Social Networks using AC2P Protocol

J.S.Harilakshmanraj
Sri Ramakrishna Engineering College, Coimbatore
Tamilnadu, India

N.Rajkumar
Sri Ramakrishna Engineering College, Coimbatore
Tamilnadu, India

Abstract: Online Social Network (OSN) sites act as a medium to spread their own views, activities and their thoughts to some camaraderie. Contents of this network are spread over web, so it was hard to determine by a human decision. Currently, they do not provide any mechanism to ensure privacy concerns towards data associated with each user. Due to this problem, number of users lacks from their ownership control. In this paper, we proposed **AC2P** (Activity Control-Access Control Protocol) for information control on the web. Alternatively, Tag Refinement strategy determines illegal tagging over images and send notification about particular image spread within different communities/groups. These techniques reduce risk of information flow and avoid unwanted tagging toward images.

Keywords: Decision based access control, Tag refinement, Online social Networking.

1. INTRODUCTION

Online Social Networks act as medium to share both personal, public information and helps to formulate network using friends, colleagues, family and even with unknown persons. It has experienced tremendous growth in recent years.Facebook is one of most frequently used social networking site, which has more than 800 million active users and over 40 billion pieces of contents like web links, news, blog posts, photos are being shared each month[2].To protect user data access control mechanism has become much needed one,[4],[5].

At present, OSN provide *user- wall* to every user, where user and their friends can post both views and content using those walls. Subsequently, users upload both content as well as *tag* other users, who appear in that content. Each tag acts an explicit reference which links to a user's space. To protect user data, OSNs require user system and policy administrator for regulating data in social network.

A simple access control mechanism allows users to govern access to information contained in their spaces, but has no control over the data, which has presented outside their spaces. For example, if a user posts a comment in a friend's space, she/he cannot specify, who should view the comment.

In another scenario,when user upload photo and tags friends who appear in the photo, he/she cannot state any privacy norms about the photo. In this paper, we propose a solution to sophisticate collaborative management of shared data in OSNs.Based on these sharing patterns, AC2P protocol is used to capture the core features of user authorization requirements that have not been accommodated, so far, By existing access control system for OSNs.(e.g.[6],[8],[9],[10]and[11]).

Accessing the implications of access control mechanisms traditionally rely on the security analysis techniques, (e.g. Operating system, [7], Trust management,[12] and role-based access control,[3] [13]).

2. BACKGROUND

At present, SNS (Social Networking Sites) allow merchants and third parties to take advantage of user information without their agreement. Some important privacy issues in SNSs are: [1],

- The privacy tool is very hard to learn and to use them, due to which people feed up and they end up doing nothing.

- User can directly control their profile information, but cannot control what others reveal about them.
- Privacy tools (or) options are desired to provide, for choosing "*Friends*", *"Friends of Friends*" (*FOF*) (or) "Everyone", but it is not yet simplified.[14].
- With the third party integration, it becomes more risky, that your information is being shared among various stakeholders,[2].

(i) Disclosing the user's identity

At present, SNSs motivates users to share profile images. So, there is a risk that propagates with technologies like Content based Image Retrieval (CBIR) by analyzing the specification of an image, which reveal details of place from where the image was taken. Most SNS users are able to share any images(or)videos regardless of who is in that specific content.So,there is a high risk of publishing user identity and location even sometimes without user knowledge.

(ii) Cyber Crime-Related Field

Some rule defines that, however vulnerable to cyber criminals who pretend themselves as a friend using fake names and gain access to all information shared by naive users.

Cutillo et al [16] state some SNS's should fulfill the following privacy requirements.

Basic Privacy Requirements: [16]

a) End-To-End Confidentiality- All communications are needed to be confidential and only the sender and receiver should have control of access to the data.

b) Privacy- Personal information of a user should not publish to any other users apart from these explicitly mentioned by the user.

c) Access Control- User should be able to manage and control over their profiles as well as attributes of their profiles.

d) Authentication- For satisfying the previous requirement of a receiver's message should be able to authenticate the sender of the message.

e) Data Integrity- For each swapped message, whether it is acknowledged or a request, original authentication and also modification detection are needed to be performed.

f) Availability- All Public data has to be accessible and all messages should be delivered in time.

3. PROBLEM DEFINITION

Major computer security aspects are: Confidentiality, Integrity and Availability. At many Social Networking Sites, have limited security protection. A developer concentrates to enhance communication between users; therefore no security threats are being identified, so far. This work identifies the threats in OSNs and finds a solution for both content sharing as well as for image tagging activities.

4. ACTIVITY CONTROL MECHANISM FOR OSNs

In this section we formalize a AC2P Protocol for OSNs (Section 4.a) as well as Decision Scheme (Section 4.b) and Decision evaluation mechanism (Section 4.c) for the specification and enforcement of privacy policies toward OSNs.

4.1 AC2P PROTOCOL MODEL

To determine the consequence of information sharing, users require good understanding towards visibility of information that to be probed. However, privacy controls in OSNs are complicated and unintuitive.

This protocol consists of three major components namely:

(i) SNS Server.
(ii) Evaluation Schema.
(iii) Host based Web Server and
(iv) Decision-Based System.

Using above components, privacy has been preserved in OSNs.

SNS Server: It Gets Request/Response from OSNs user. Appropriate request messages are transmitted to application servers and it gets a notification from the application server (Alert-MSG), based on the user decision, particular OSN content will be allowed for other user's visibility.

Evaluation Schema: It verifies the content and check whether it is unique (or) not. It acts as *Plagiarism checker* to validate the uniqueness.

Host based Web server: It acts as authentication measurement system. If user blocks visibility of content to particular users. Then level of privileges is being measured for each and every user. Measurements are done in forms of

(i) High-Risk
(ii) Intermediate-Risk
(iii) No-Risk.

Decision-based System: An OSNs user has direct control over to set privacy. This component offers two ways of decision making towards the content:

- ➢ Allow the content (Others Visibility)
- ➢ Refuse the content(DENY)

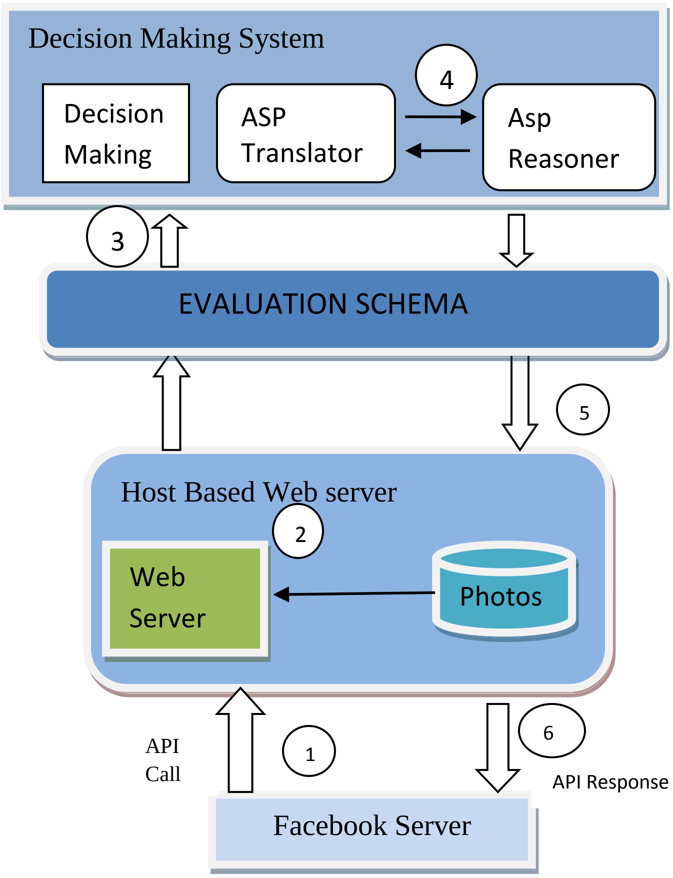


Fig.4.1 Framework of AC2P Protocol.

In fig 4.1 describe about components and strategies involved in AC2P Protocol mechanism, which used to protect OSNs contents from unauthorized users. It follows certain procedures, is being stated below:

1. *API call procedure*- it intimates host server whether to share the content or not.
2. *An Access request*- Notification is sent to the Evaluation mechanism (Section 4.3).
3. Examining the uniqueness of OSNs content is done.
4. After evaluation, *Final decision* is taken.
5. The Final decision will be either to "*Allow*" or "*Deny*" the OSNs content.
6. Using, the *API Response* final decision is notified to FB server.

4.2 EVALUATION SCHEMA

This schema used to predict the uniqueness of content in OSNs. For Example, if Bob post some content in public-view, john see that content as well as trim some information and post to his wall. In above scenario, some modification is been done towards the content. To predict that activity in OSNs, this schema used to predict the uniqueness value and send notification to particular user about their content was been access by other user, whether content should allowed or not. Alert notification is been generated.

4.3 *PROTOCOL -POLICY SPECIFICATION*

In Fig 4.2.,a disseminator used to share other profile information to others. So this kind of access specific schemas is being used widely [17][18].By using this kind of access privacy setting and access control norms will not be suitable for a privacy protection scenario. Some modification needs to be done.By using single controller, the resource-owner, to specify access control policies. A policy evaluation scheme is used to evaluate the DV (Decision-Value).A DV value state two possibilities either "Allow" or "Deny". This decision is taken based on some constraints.

$$\text{Decision}= \begin{cases} \text{Permit} \quad \text{if } \mathit{DV}\text{ag} > \text{Sc.} \\ \text{Deny} \quad \text{if } \mathit{DV}\text{ag} \leq \text{Sc} \;.....(1) \end{cases}$$

If the Sc is high, there is a chance of *Deny* access, take cares of high sensitive data.otherwise, the final verdict is most likely to *Allow* the data access.

(i) Owner-overrides: The owner decision is the final decision, It has highest priority. Based on the weight age of decision making scheme, we set w_{ow}=1, w_{cb}=0,then

$$\text{Decision}= \begin{cases} \text{Permit, if DVag=1} \\ \text{Deny, if DVag=0} \;.......(2) \end{cases}$$

(ii) Majority-Permit: The sending request is greater than the number of controller to deny, the final decision will be

$$\begin{cases} \text{Permit, if DVag} \geq ½ \end{cases}$$

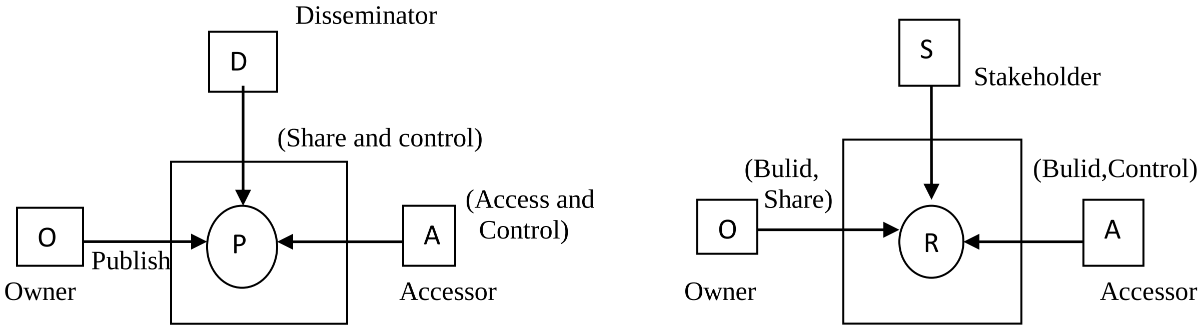
Decision= Deny, if $DV_{ag} < \frac{1}{2}$ ….(3)

By using the above strategies, owner (U*i*) Will take the final decision to *Allow* (or) *Deny* the data object.

4.4 *DECISION EVALUATION MECHANISM*

To make an authorized decision from the user(U*i*) of content policy evaluation schema used for decision making purpose.It makes privacy setting based on certain norms desired by an owner(U*i*), In fig.4.3 illustrate overall scenario of access mechanism and its functionalities. Decision aggregate is being generalized and not been specialized under some constraints, but determines whether to *refuse* (or) to *allow* the content.

The probability flow model (*PFM*) used to predict,whether the user(U*j*) will get permission for content from the owner(U*i*).It is important to notify that OSNs community is defined for each and every user separately.Some sub-community use to define particular contexts.It is also possible to develop aggregations of OSN community in Social Neighborhood(SN) to form own communities. Using this model, some evaluation is being done. We used to collect some benchmark datasets from Facebook.Using, those datasets some evaluation are been done.



a) A Disseminator shares other profile

b) A user shares his/her relationships

FIG 4.2. Profile and Personal information Sharing schema is being processed.Based on the hop value and community value(C*i*),the distribution size is being calculated.

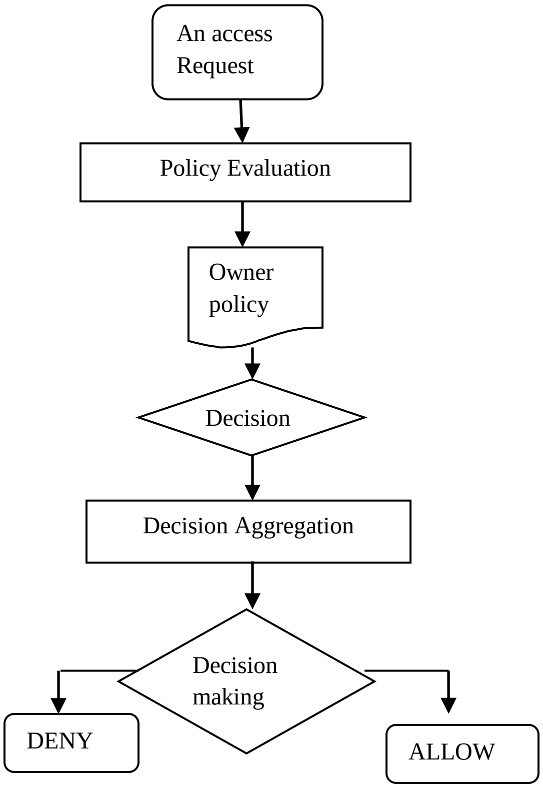


FIG.4.3 Schematic structure of Decision Evaluation Mechanism

4.4.1 A Voting Schema for Decision-Making

Various types of voting schemas are used for decision making [19].We proposes a voting scheme to achieve an effective user based conflict resolution in OSNs.Our voting schema consists two voting mechanisms.

- ***(i)*** **Decision based voting.**
- ***(ii)*** **Sensible voting.**

Decision based voting: A decision value (*DV*) is enhanced from the policy evaluation is defined as follows, where Evaluation *(P*) returns the decision of a Policy (*p).*

$$\text{Decision}=\begin{cases} 0 & \text{if Evaluation (p) =Deny} \\ 1 & \text{if Evaluation (p) =Permit… (4)} \end{cases}$$

Sensible voting: Each user assigns an SL to the shared data item to reflect her/his privacy concern. A sensitivity score (Sc) (in the range from 0.00 to 1.00) for the data item can be calculated based on the following equation:

$$S_c= (SL_{ow}+SL_{cb}+\textstyle\sum_{i\varepsilon SS} SL^{i}{}_{st}) \text{ x } \frac{1}{m}\text{..........(5)}$$

5. Tag Refinement Strategy

If user were tagged in particular photo, user can ensure privacy control to the particular photograph. Customized access permission is used to control and avoid undesired tagging towards photograph. In fig 5.a., states the complete scenario and overall behavior of Access customization towards tagging image.

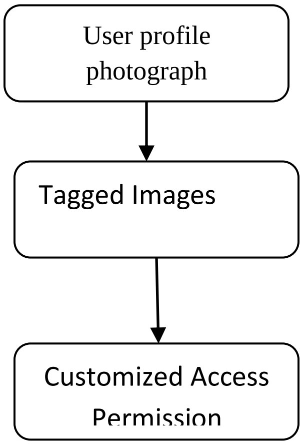
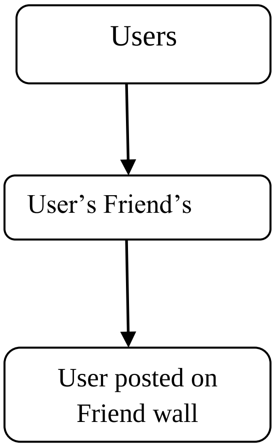


Fig 5.1 Access Customization over Tagged Images

5.2 Visibility Control Policy

If users post any message on a public wall, then the visibility of that post is governed as per the privacy policies of the user on whose wall we posted. However, In some situations user who is posting may want to control who among our common friends can view that post. This policy enables us to allow/disallow users among our common friends to view our post. It has been enabled by Access control schema.



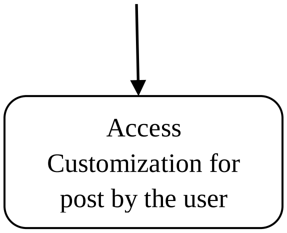


Fig 5.2 Visibility Control Policy

6. Evaluation Of Access Control Mechanism

A VisibilityControlList (VCL) is being used for the evaluation process. It is an enhancement of ACL (Access Control List) which used to state the privacy-level of each user and it state the privileges assigned to each individual user.

Blog_ID	Allow	Deny
1	✓	×
2	×	×
3	✓	✓
4	×	✓

Table 6 Visibility Access List

Based on VCL access permissions-whether to “Block “or “Deny “ the user for appropriate content accessing over OSN.In fig 5.a Evaluation result indicates the level of privacy towards contents that was being preserved by AC2P Protocol .

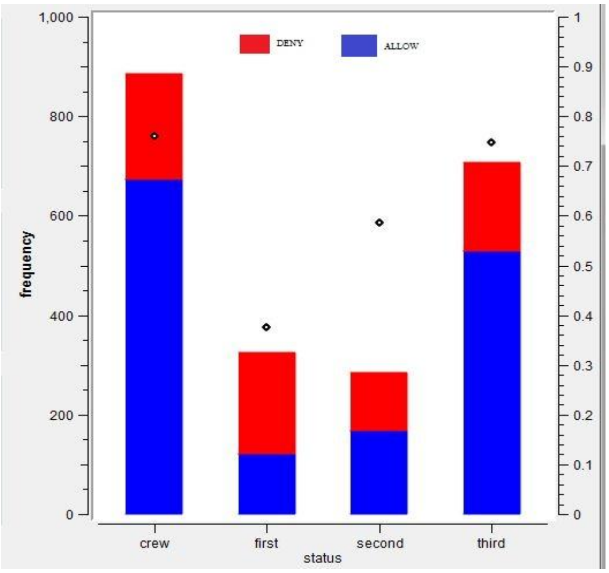


Fig 6.1 Analyzing of DCAM model.

In Fig 5.a, overall performance of a AC2P Protocol is evaluated based using (DV) value. This value is used for the prediction over OSN content.

6.1 Performance Evaluation

Based on the contents, which was shared between users, are determined on the basis of *outflow* and *inflow* strategy. It is determined using some constraint equ(6).

$$C_i = \begin{cases} \text{Outflow/Inflow} & \text{Outflow} < \text{Inflow} \\ 1 & \text{Outflow} > \text{Inflow} \ldots\ldots..(6) \end{cases}$$

Outflow = the number of interactions, user U*i* has with her friend.

Inflow = the number of interactions U*i’s* friends

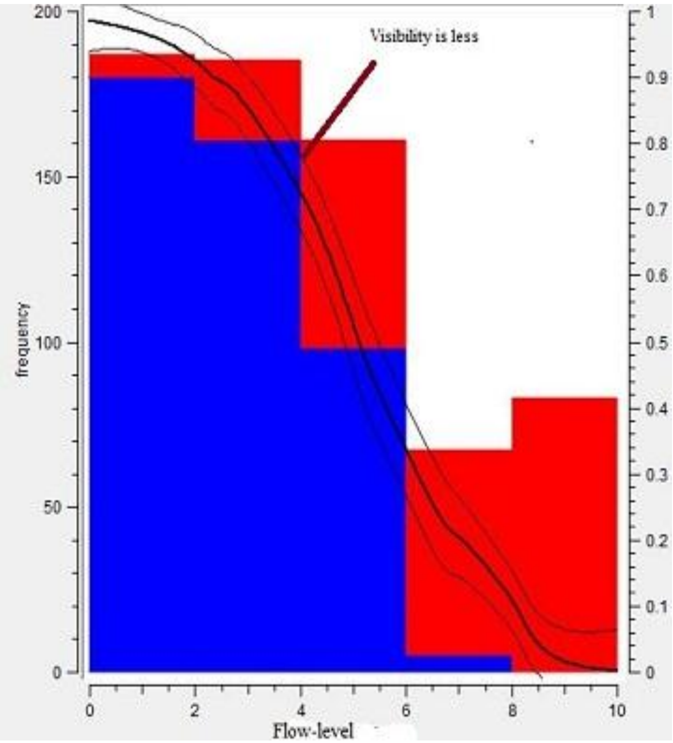


Fig 6.2 Probing the risk of leakage over OSNs contents

Finally, AC2P Protocol reduces risk of information leakage and assures ownership policy over user (U*i*).Above fig 6.b state the privacy-level managed using DCAM model.

7. CONCLUSION

In this paper, we has been proposed a better solution for both illegal content accessing of shared data and unwanted image tagging on OSNs. AC2P protocol was developed with Decision Scheme and Decision evaluation mechanism. In addition, we have introduced an approach for representing and reasoning about our proposed model.Tag Refinement is being proposed to avoid unwanted tagging and it preserve user and ensure ownership.So,user can make the decision to allow/disallow users among our common friends to view our post.

8. FUTURE WORK

In future work, we are planning to determine the comprehensive privacy conflict resolution approach[21],[22]and to probe the services of collaborative management of shared data in OSN's.We would study inference-based techniques [20] for automatically configure privacy preferences in the AC2P Protocol. Besides, we plan to systematically integrate the notion of trust and reputation into Decision making model and investigate a comprehensive solution to cope with collusion attacks for providing a robust Decision making service in OSNs.

REFERENCES

[1] Mark Hachman (April 23,2012). "Facebook Now Totals 1.20 billion Users, Profits Slip". PCMag.com. Retrieved September 24, 2013.

[2] Facebook Statistics, http://www.facebook.com/ Press/ info .php?statistics, 2013.

[3] G. Ahn and H. Hu, "Towards Realizing a Formal RBAC model in Real Systems," Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 215-224, 2007.

[4] Facebook Privacy Policy, http://www.facebook.com/policy.php/, 2013.

[5] Google+ Privacy Policy, http://http://www.google.com/intl/en/+/policy/, 2013.

[6] B. Carminati, E. Ferrari, and A. Perego, "Rule-Based Access Control for Social Networks," Proc. Int'l Conf. On the Move to Meaningful Internet Systems, pp. 1734-1744, 2006.

[7] M. Harrison, W. Ruzzo, and J. Ullman, "Protection in Operating Systems," Comm. ACM, vol. 19, no. 8, pp. 461-471, 1976.

[8] B. Carminati, E. Ferrari, and A. Perego, "Enforcing Access Control in Web-Based Social Networks," ACM Trans. Information and System Security, vol. 13, no. 1, pp. 1-38, 2009.

[9] P. Fong, "Relationship-Based Access Control: Protection Model and Policy Language," Proc. First ACM Conf. Data and Application Security and Privacy, pp. 191-202, 2011.

[10] P. Fong, M. Anwar, and Z. Zhao, "A Privacy Preservation Model for Facebook-Style Social Network Systems," Proc. 14th European Conf. Research in Computer Security, pp. 303-320, 2009.

[11] S. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and H. Choi "D-FOAF: Distributed Identity Management with Access Rights Delegation," Proc. Asian Semantic Web Conf. (ASWC), pp. 140-154,2006.

[12] N. Li, J. Mitchell, and W. Winsborough, "Beyond Proof-of- Compliance: Security Analysis in Trust Management," J. ACM,vol. 52, no. 3, pp. 474-514, 2005.

[13] H. Hu and G. Ahn, "Enabling Verification and Conformance Testing for Access Control Model," Proc. 13th ACM Symp. Access Control Models and Technologies, pp. 195-204, 2008.

[14] Aimeur, E.; gambus,S.; Ai Ho; , "UPP: User Privacy Policy for Social Networking Sites,"Internet and Web Applications and Services,2009. ICIW '09.Fourth International Conference on vol., no., pp.267-272,24-28 May 2009.

[15] A. Ho, A4. Maiga, and E. Aimeur, "Privacy protection issues in social networking sites,"IEEE/Acs International Conference on Computer Systems and Applications 2009 (AICCSA 2009),PP.271-278,Country,2009

[16] SeyedHossein Mohtasebi and Ali Dehghantanha," A Mitigation Approach to the Malwares Threats of Social Network Services," Muktimedia Information Networking and Security,2009. MINES'09. International Conference on, vol.1,no.,pp.448-459,2011

[17] B. Carminati, E. Ferrari, and A. Perego, "Rule-Based Access Control for Social Networks," Proc. Int'l Conf. On the Move to Meaningful Internet Systems, pp. 1734-1744, 2006.

[18] P. Fong, "Relationship-Based Access Control: Protection Model and Policy Language," Proc. First ACM Conf. Data and Application Security and Privacy, pp. 191-202, 2011.

[19] L. Lam and C.Y. Suen, "Application of Majority Voting to Pattern Recognition: An Analysis of Its Behavior and Performance," IEEE Trans. Systems, Man and Cybernetics, Part A: Systems and Humans, vol. 27, no. 5, pp. 553-568, Sept. 1997.

[20] A. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, "A3p: Adaptive Policy Prediction for Shared Images over Popular Content Sharing Sites," Proc. 22nd ACM Conf. Hypertext and Hypermedia, pp. 261-270, 2011.

[21] H. Hu, G. Ahn, and K. Kulkarni, "Anomaly Discovery and Resolution in Web Access Control Policies," Proc. 16th ACM Symp.Access Control Models and Technologies, pp. 165-174, 2011.

[22] H. Hu, G.-J. Ahn, and K. Kulkarni, "Detecting and Resolving Firewall Policy Anomalies," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 3, pp. 318-331, May 2012.

Mr.J.S.HARILAKSHMANRAJ, Student at Department of Software Engineering at Sri Ramakrishna engineering college, Tamilnadu.He received Bachelor Degree from Kumaraguru college of Technology, Tamilnadu.His research interest focus on Social Network Analysis, Data Mining and Web-mining.

Dr.N.RAJKUMAR,Head of department of M.E. Software Engineering, at Sri Ramakrishna Engineering College, Tamilnadu. He received Ph.D Degree at Bharathiyar University during 2005.His specialization was Datamining, webmining.