IJMTST is UGC Approved Journal with Journal Id: 43137

International Journal for Modern Trends in Science and Technology, 8(S08): 179-184, 2022
Copyright © 2022 International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST08S0831
Available online at: https://www.ijmtst.com/vol8si08.html

Check for updates

CCP-CABE Framework model to protect privacy for information sharing in OSN's

Dr. D J Samatha Naidu[1] | M.Sowjanya[2]

Principal, Annamacharya PG college of computer studies, Rajampet.
Annamacharya PG college of computer studies, Rajampet.

To Cite this Article
Dr. D J Samatha Naidu and M.Sowjanya. CCP-CABE Framework model to protect privacy for information sharing in OSN's. International Journal for Modern Trends in Science and Technology 2022, 8(S08), pp. 179-184. https://doi.org/10.46501/IJMTST08S0831

Article Info
Received: 26 May 2022; Accepted: 24 June 2022; Published: 28 June 2022.

ABSTRACT

Internet users receive various online social network (osns)services, however, provides of osns do not always provide users fine -gained privacy protection for shared resources. A growing need of information sharing and the new development of the internet, there is a strong demand of new security models for personal information protection when people share information. In this project presented the ogbac model to meet the need of privacy protection in social network information sharing application. The locarative survey of the related studies to find the limitations in existing privacy mechanisms of osns. Based on the survey findings proposed the ogbac model which combines the classic access control model with the information flow control policies. This model can ensure that the sharing information flows within or among own groups according to the partial ordering of osns environmental attributes (such as security level, semantic tag and. Effective time period).to implement the model with ccp-cabe to demonstrate the effectiveness of the model. The security and other performance of the model as well as the implemented system are analyzed. Our model could be improved in terms of efficiency and accuracy when deployed in real word applications. The social networks are much more complex than the operating system and other environments where traditional access control policies are used. the methods of information flow cannot solve the problems like instructed nodes. Some own users do not have care about the access control policies. Administration related rules and access related rules are designed for each access operation of group based osns information sharing. The security of ogbac model is analyzed using formal methods to ogbac model is analyzed using formal methods. To demonstrate the usability of the ogbac based encryption (ccp-cabe), and analyze the security and efficiency of the implemented system to prove the effectiveness of the implemented system.

KEYWORDS: introduction, related work, , modules and discription,screens

1. INTRODUCTION

NLINE Social Networks (OSNs), such as Twitter, Flickr, Facebook, MySpace, LinkedIn and WeChat, have developed a huge number of Internet users over the past years. OSN users contact each other for various purposes including friendship, entertainment, social experience and knowledge sharing. In order to help users protect their private personal information, current OSNs often adopt a simple user-centric policy management mechanism which requires users to specify policies for managing access to their posted resources [1]. However, this mechanism mainly focuses on attaching attributes and policies to an should not have access to the object [2]. The insecure information flow comes from the interrelated OSNs' nodes which are connected by weak relationship in the virtual environment. If Alice becomes a friend of Bob in an OSN, Alice can access information from Bob's friends. Bob's friends may repost Bob's early posts some of which Bob does not want Alice to know. The access control models used in current OSNs cannot make users determine which friends can access what resources during what time accurately and dynamically. As a result, sensitive information may be disseminated to unwanted users. Furthermore, if a user does not realize the importance of protecting privacy and makes the private personal information known to the public, the information may be easily disseminated to malicious attackers, which may further cause illegal or criminal results. Users in an OSN usually form organizations with relatively stable members, clear social tags and boundaries, called “groups” [3]. Recently, with more and more people joining in OSNs, it is popular to share information and ideas within and among OSN groups. For example, it is reported that every day, about 2,300,000 new groups are created in WeChat [4], the most popular OSN in China. It is very common for ordinary people in China to share various types of information through such kind of OSN groups. For OSNs, one user may have dozens to hundreds of groups, and the new shared information (like a picture or news) posted by a member of one group can be reposted to another group by members who belong to both groups. Due to the huge number of the members of a group as well as the total number of groups, we believe this kind of inter-group OSNs information sharing and dissemination can sharply enlarge the risk of information disclosure. Such risk may prevent the users from sharing useful information in OSN groups [5], defeating the purpose of OSNs in sharing information, exchanging the experiences, strengthening friendships and flourishing the culture of human beings.

2.EXISTING WORK

Vyas et al. [11] studied the use of annotation data to predict users’ privacy preferences and automatically derived policies for shared content based on a semantic analysis of tags. Squicciarini et al. [12] developed an Adaptive Policy Prediction (A3P) system to help users compose privacy settings for their online images. Zerr et al. [13, 14] developed a search engine for privacy oriented image search as well as a web service for supporting user decisions regarding image privacy. Squicciarini et al. [15] conducted a comprehensive study on large-scale image privacy classification which includes not only simple privacy classification models based on binary labels, but also models for more complex and multi-facet privacy settings. Hu et al. [16] proposed a framework of calculating the privacy level of a digital image based on perceptual hashing and semantic privacy rules. The calculated privacy level can be fed to the user before he/she shares the image to OSNs, and also can be used as a valuable reference for the design of more finegrained OSNs’ access control systems.

Carminati et al. [17] proposed an extensible OSN access control model based on semantic web technologies. The main idea is to encode social networkrelated information by means of ontology. Squicciarini et al. [1] applied the game theory to model the problem of collective enforcement of privacy policies on shared data in OSNs. Shehab et al. [18] presented an access control framework to prevent the OSN applications from accessing user’s personal data. Li et al. [19] investigated the effectiveness of privacy control mechanisms against privacy leakage from the perspective of information flow. The analysis revealed that the existing privacy control mechanisms do not protect the flow of personal information effectively. The authors also provided suggestions or remedies for OSN users to mitigate the risk of involuntary information leakage in OSNs.

DISADVANTAGES

- In the existing work, the system did not implement Group-Based Access Control (oGBAC) framework which leads very less effective
- This system is less performance due to lack of Attribute based encryption techniques.

2.3.2. PROPOSED WORK WITH ADVANTAGES

In the proposed oGBAC, the system imposes some restrictions to the information flow among groups to ensure that operations cannot incur privacy disclosure when sharing information among friends in OSNs. In view of characteristics of OSNs and the requirements of secure information flow, the oGBAC incorporates some ideas from the Attribute-Based Access Control (ABAC) to develop information flow-based.rules using relationship among attributes (such as tags, time and security levels) of objects and subjects in OSNs. We implement the model with the Comparative Attribute-Based Encryption (CCP-CABE), and achieve the objective of eachoGBAC policy with cryptography algorithms. It is very hard to attack the CCP-CABE, so the security condition of each oGBAC policy is assured in the implementation. We analyze the security of the oGBAC model with information flowtheorems, and also analyze the security and efficiency of the CCP-CABE based implementation system.

ADVANTAGES

- The system is more effective due to presence of Ciphertext-Policy Attribute-Based Encryption (CP-ABE).
- The system is Group-Based Access Control (oGBAC) framework which for preventing security violation and privacy disclosure when sharing information within or among groups in OSNs.

3. MODULES AND ITS DESCRIPTION

1.Data owner

In this module, the data owner should register by providing user name, password, email and group, after registering owner has to Login by using valid user name and password. The Data owner browses and uploads their data to the cloud server. For the security purpose the data provider encrypts the data file and then stores in the web server.

2. Group Authority

The group authority is responsible for registering and login authorization for the end users if they are in the same group and also

1.view group users 2.view group signs 3.Registerd user

3.Storage Server

The Storage server is responsible for data storage and file authorization for an end user. The data file will be stored in cloud server with their tags such as Owner, file name, secret key, mac and private key, can also view the registered Owners and End-users in the cloud server. The data file will be sending based on the privileges. If the privilege is correct then the data will be sent to the corresponding user and also will check the file name, end user name and secret key. If all are true then it will send to the corresponding user or he will be captured as attacker.

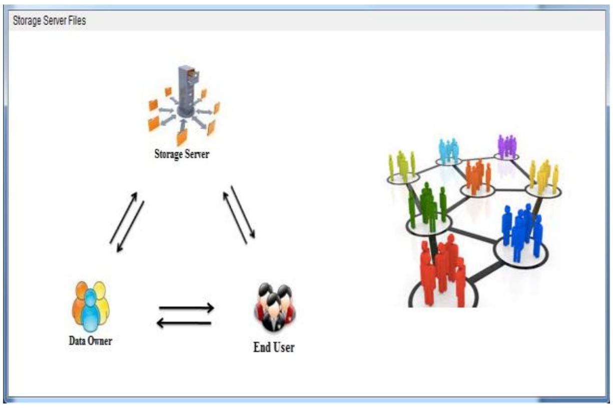
4.Data Consumer(End User)

The data consumer is nothing but the end user who will request and gets file contents response from the corresponding cloud servers. If the file name and secret key, access permission like Search and download icorrect then the end is getting the file response from the cloud or else he will be considered as an attacker and also he will be blocked in corresponding cloud. If he wants to access the file after blocking he wants to UN block from the cloud.

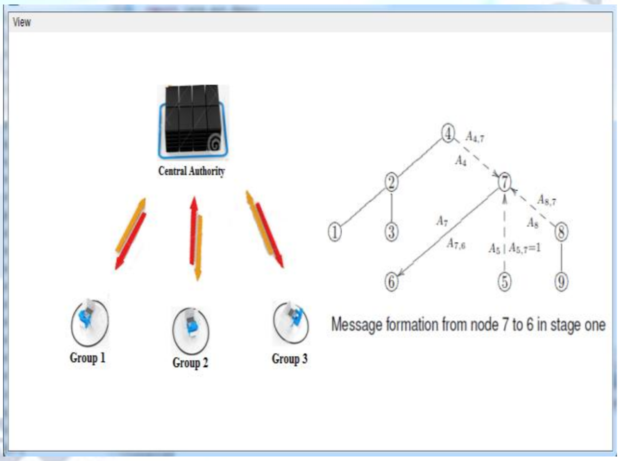
5.Attacker

Threat model is one who is trying to receive files by giving fake Skey to the file in the Storage Server. The attacker may be within a Network or from outside the network. If attacker is from inside the network then those attackers are called as internal attackers. If the attacker is from outside the network then those attackers are called as external attackers.

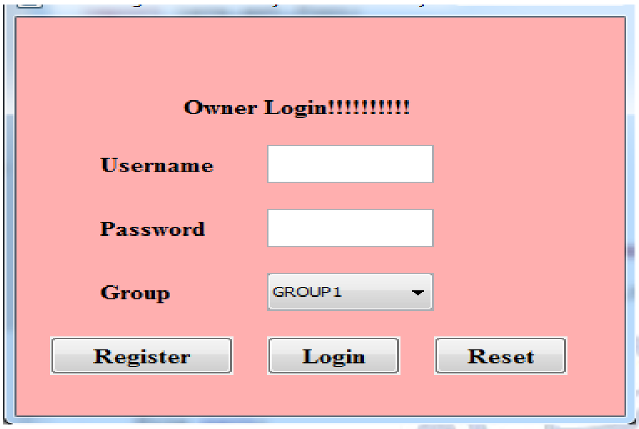
4 SIMULATION RESULTS:



Screen 1. Storage Server



Screen 2. Group Authority



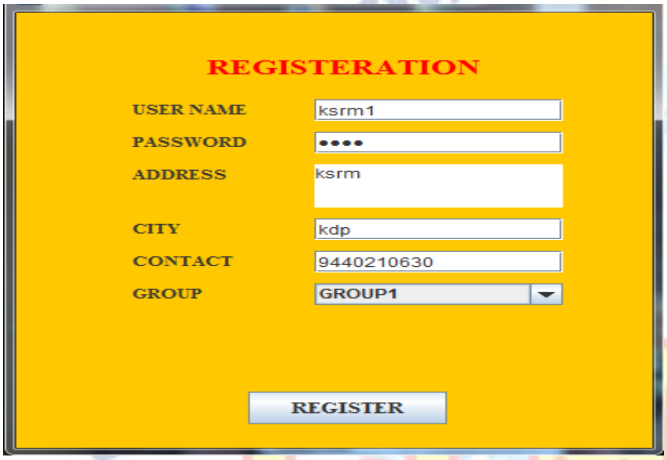
Owner Login!!!!!!!!!!

Username

Password

Group GROUP1

Screen 3. Owner Login



REGISTERATION

USER NAME ksrm1

PASSWORD ●●●●

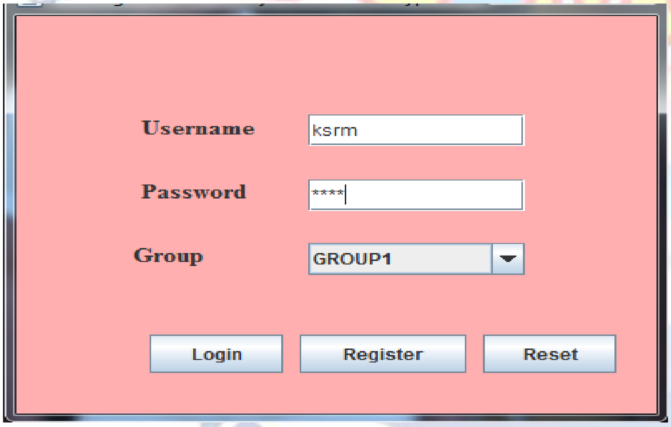
ADDRESS ksrm

CITY kdp

CONTACT 9440210630

GROUP GROUP1

Screen 4. User Registration

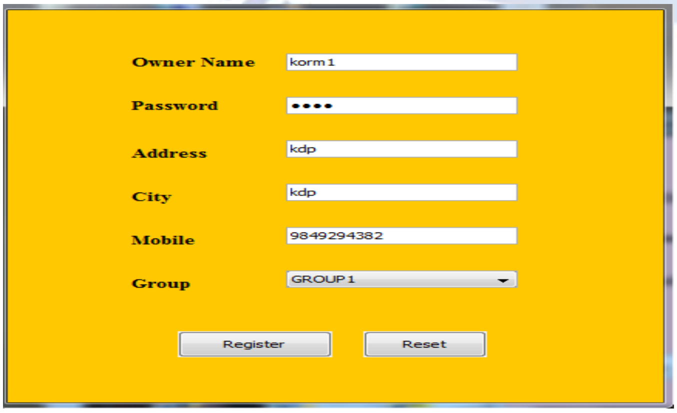


Username ksrm

Password ****

Group GROUP1

Screen 5. User Login



Owner Name korm1

Password ●●●●

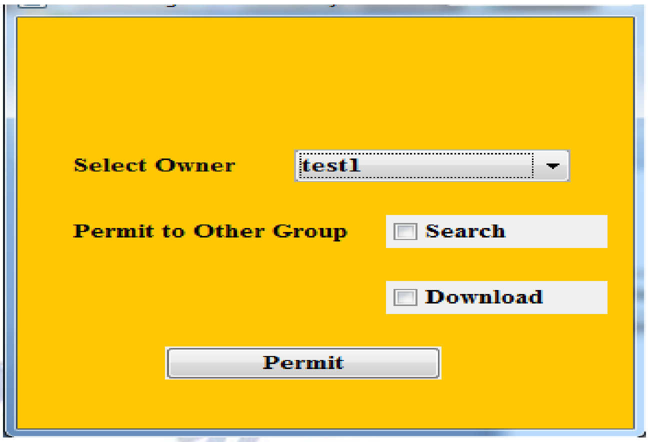
Address kdp

City kdp

Mobile 9849294382

Group GROUP1

Screen 6. Owner Registrar

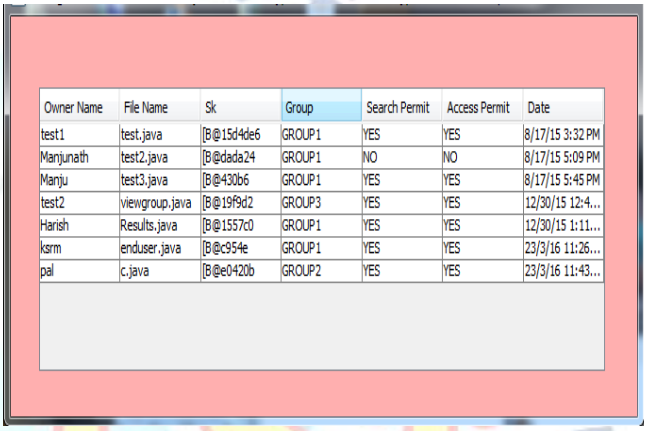


Select Owner test1

Permit to Other Group □ Search

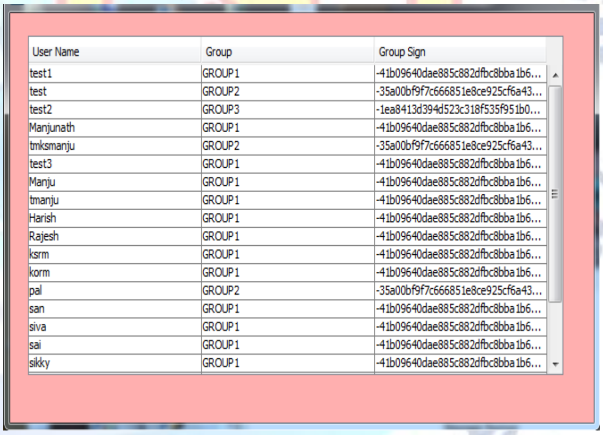
□ Download

Screen 7. Give Privilages



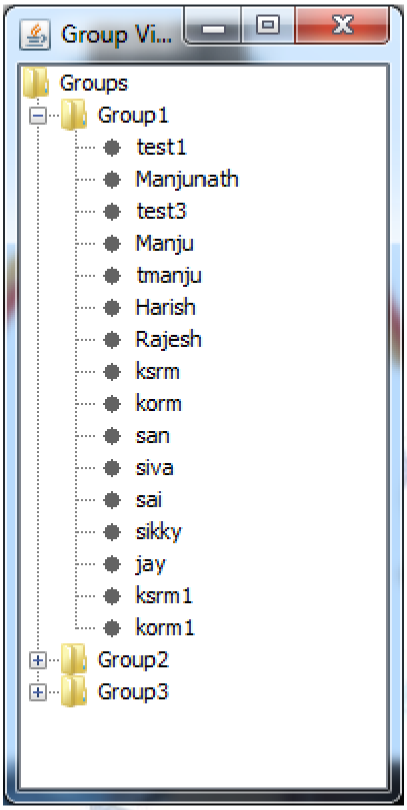
Owner Name	File Name	Sk	Group	Search Permit	Access Permit	Date
test1	test.java	[B@15d4de6	GROUP1	YES	YES	8/17/15 3:32 PM
Manjunath	test2.java	[B@dada24	GROUP1	NO	NO	8/17/15 5:09 PM
Manju	test3.java	[B@430b6	GROUP1	YES	YES	8/17/15 5:45 PM
test2	viewgroup.java	[B@19f9d2	GROUP3	YES	YES	12/30/15 12:4...
Harish	Results.java	[B@1557c0	GROUP1	YES	YES	12/30/15 1:11...
ksrm	enduser.java	[B@c954e	GROUP1	YES	YES	23/3/16 11:26...
pal	c.java	[B@e0420b	GROUP2	YES	YES	23/3/16 11:43...

Screen 8. Storage Server Files



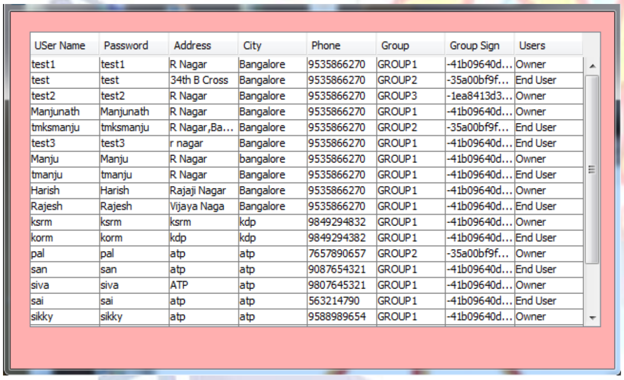
User Name	Group	Group Sign
test1	GROUP1	-41b09640dae885c882dfbc8bba1b6...
test	GROUP2	-35a00bf9f7c666851e8ce925cf6a43...
test2	GROUP3	-1ea8413d394d523c318f535f951b0...
Manjunath	GROUP1	-41b09640dae885c882dfbc8bba1b6...
tmksmanju	GROUP2	-35a00bf9f7c666851e8ce925cf6a43...
test3	GROUP1	-41b09640dae885c882dfbc8bba1b6...
Manju	GROUP1	-41b09640dae885c882dfbc8bba1b6...
tmanju	GROUP1	-41b09640dae885c882dfbc8bba1b6...
Harish	GROUP1	-41b09640dae885c882dfbc8bba1b6...
Rajesh	GROUP1	-41b09640dae885c882dfbc8bba1b6...
ksrm	GROUP1	-41b09640dae885c882dfbc8bba1b6...
korm	GROUP1	-41b09640dae885c882dfbc8bba1b6...
pal	GROUP2	-35a00bf9f7c666851e8ce925cf6a43...
san	GROUP1	-41b09640dae885c882dfbc8bba1b6...
siva	GROUP1	-41b09640dae885c882dfbc8bba1b6...
sai	GROUP1	-41b09640dae885c882dfbc8bba1b6...
sikky	GROUP1	-41b09640dae885c882dfbc8bba1b6...

Screen 10. Registered Users



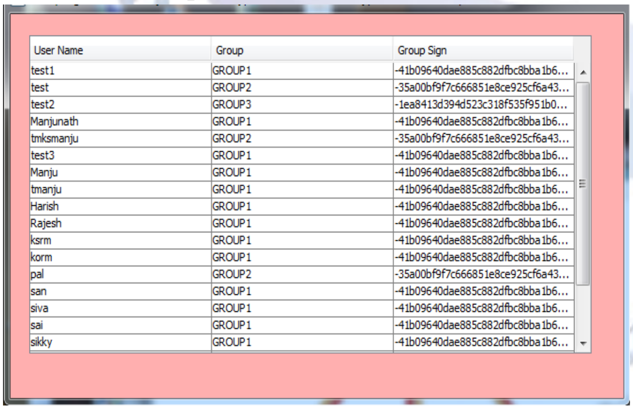
Groups
- Group1
  - test1
  - Manjunath
  - test3
  - Manju
  - tmanju
  - Harish
  - Rajesh
  - ksrm
  - korm
  - san
  - siva
  - sai
  - sikky
  - jay
  - ksrm1
  - korm1
- Group2
- Group3

Screen 11.9. Group Details



USer Name	Password	Address	City	Phone	Group	Group Sign	Users
test1	test1	R Nagar	Bangalore	9535866270	GROUP1	-41b09640d...	Owner
test	test	34th B Cross	Bangalore	9535866270	GROUP2	-35a00bf9f...	End User
test2	test2	R Nagar	Bangalore	9535866270	GROUP3	-1ea8413d3...	Owner
Manjunath	Manjunath	R Nagar	Bangalore	9535866270	GROUP1	-41b09640d...	Owner
tmksmanju	tmksmanju	R Nagar,Ba...	Bangalore	9535866270	GROUP2	-35a00bf9f...	End User
test3	test3	r nagar	Bangalore	9535866270	GROUP1	-41b09640d...	End User
Manju	Manju	R Nagar	bangalore	9535866270	GROUP1	-41b09640d...	Owner
tmanju	tmanju	R Nagar	Bangalore	9535866270	GROUP1	-41b09640d...	End User
Harish	Harish	Rajaji Nagar	Bangalore	9535866270	GROUP1	-41b09640d...	Owner
Rajesh	Rajesh	Vijaya Naga	Bangalore	9535866270	GROUP1	-41b09640d...	End User
ksrm	ksrm	ksrm	kdp	9849294832	GROUP1	-41b09640d...	Owner
korm	korm	kdp	kdp	9849294382	GROUP1	-41b09640d...	End User
pal	pal	atp	atp	7657890657	GROUP2	-35a00bf9f...	Owner
san	san	atp	atp	9087654321	GROUP1	-41b09640d...	End User
siva	siva	ATP	atp	9807645321	GROUP1	-41b09640d...	Owner
sai	sai	atp	atp	563214790	GROUP1	-41b09640d...	End User
sikky	sikky	atp	atp	9588989654	GROUP1	-41b09640d...	Owner

Screen 11. Group View



User Name	Group	Group Sign
test1	GROUP1	-41b09640dae885c882dfbc8bba1b6...
test	GROUP2	-35a00bf9f7c666851e8ce925cf6a43...
test2	GROUP3	-1ea8413d394d523c318f535f951b0...
Manjunath	GROUP1	-41b09640dae885c882dfbc8bba1b6...
tmksmanju	GROUP2	-35a00bf9f7c666851e8ce925cf6a43...
test3	GROUP1	-41b09640dae885c882dfbc8bba1b6...
Manju	GROUP1	-41b09640dae885c882dfbc8bba1b6...
tmanju	GROUP1	-41b09640dae885c882dfbc8bba1b6...
Harish	GROUP1	-41b09640dae885c882dfbc8bba1b6...
Rajesh	GROUP1	-41b09640dae885c882dfbc8bba1b6...
ksrm	GROUP1	-41b09640dae885c882dfbc8bba1b6...
korm	GROUP1	-41b09640dae885c882dfbc8bba1b6...
pal	GROUP2	-35a00bf9f7c666851e8ce925cf6a43...
san	GROUP1	-41b09640dae885c882dfbc8bba1b6...
siva	GROUP1	-41b09640dae885c882dfbc8bba1b6...
sai	GROUP1	-41b09640dae885c882dfbc8bba1b6...
sikky	GROUP1	-41b09640dae885c882dfbc8bba1b6...

Screen 11.12. Group Sign

5. CONCLUSION

With a growing need of information sharing and the new development of the Internet, there is a strong demand of new security models for personal information protection when people share information. In this paper, we presented the oGBAC model to meet the need of privacy protection in social network information sharing applications. We have conducted a survey of the related studies to find the limitations in existing privacy mechanisms of OSNs. Based on the survey findings, we proposed the oGBAC model which combines the classic access control model with the information flow control policies. This model can ensure that the sharing information flows within or among OSN groups according to the partial ordering of OSNs' environmental attributes (such as security level, semantic tag and effective time period). We implement the model with CCP-CABE to demonstrate the effectiveness of the model. The security and other performance of the model as well as the implemented system are analyzed. Our model could be improved in terms of efficiency and accuracy when deployed in real-world applications. The social networks are much more complex than the operating system and other environments where traditional access control policies are used. The methods of information flow cannot solve the problems like untrusted nodes

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] J. Kivinen and M. K. Warmuth, “Additive versus exponentiated gradient updates for linear prediction,” in Proc. 27th Annu. ACM Symp. Theory Comput., 1995, pp. 209– 218.

[2] T. L. Griffiths and M. Steyvers, “Finding scientific topics,” Proc. Nat. Acad. Sci. USA, vol. 101, pp. 5228–5235, 2004.

[3] A. Klementiev, D. Roth, and K. Small, “An unsupervised learning algorithm for rank aggregation,” in Proc. 18th Eur. Conf. Mach. Learn., 2007, pp. 616–623.

[4] Y.-T. Liu, T.-Y. Liu, T. Qin, Z.-M. Ma, and H. Li, “Supervised rank aggregation,” in Proc. 16th Int. Conf. World Wide Web, 2007, pp. 481–490.

[5] G. Heinrich, Parameter estimation for text analysis, “ Univ. Leipzig, Leipzig, Germany, Tech. Rep., http://faculty.cs.byu.edu/~ringger/ CS601R/papers/Heinrich-GibbsLDA.pdf, 2008.

[6] A. Klementiev, D. Roth, and K. Small, “Unsupervised rank aggregation with distance-based models,” in Proc. 25th Int. Conf. Mach. Learn., 2008, pp. 472–479.

[7] N. Jindal and B. Liu, “Opinion spam and analysis,” in Proc. Int. Conf. Web Search Data Mining, 2008, pp. 219–230.

[8] A. Klementiev, D. Roth, K. Small, and I. Titov, “Unsupervised rank aggregation with domain-specific expertise,” in Proc. 21st Int. Joint Conf. Artif. Intell., 2009, pp. 1101–1106.

[9] E.-P. Lim, V.-A. Nguyen, N. Jindal, B. Liu, and H. W. Lauw, "Detecting product review spammers using rating behaviors," in Proc. 19thACMInt. Conf. Inform. Knowl. Manage., 2010, pp. 939–948.

[10] Y. Ge, H. Xiong, C. Liu, and Z.-H. Zhou, "A taxi driving fraud detection system," in Proc. IEEE 11th Int. Conf. Data Mining, 2011, pp. 181–190.

[11] D. F. Gleich and L.-h. Lim, "Rank aggregation via nuclear norm minimization," in Proc. 17th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2011, pp. 60– 68.