iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** XII **Month of publication:** December 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Multiparty Authorization for Online Social Network

Prof. Subhash V. Pingale [#1], Sandip Sharad Shirgave [*2]
[#]*Department Of Computer Engineering*
SKN Sinhgad College of Engineering
Korti, Pandharpur, India-413 304

Abstract— Web-based online social networks (WBOSNs) are online communities where participants or users can share information and resources with each other with known users and unknown users. In current online social networks users are connected with each other, they share their personal and public information over the network. Online social networking sites having main role in connecting the peoples over the world. In recent years, most of the online social networks are adopting the semantic web technologies such as Friend-of-a-friend (FOAF) for showing online users private and public data and relationship , making it possible to enforce data and information resources across multiple web based online social network. In this paper we are presenting an access control model for web based social network, where we give the access to the multiple users for controlling their privacy in social network.
Keywords— social network, access control model, online users, privacy

I. INTRODUCTION

In the web based online social network there are online groups and communities which allows user to publish data ,information and to establish relationships with other online users, that online user may be different type (college friend, school friend or roommate) for purposes which may concern for example entertainment, religion, dating, or business. Online social networks (OSNs) such as Facebook, Twitter, and Google+ are essentially designed to facilitate people to share personal and public information and formulate social relations with friends, colleagues, family, and co-workers and even with strangers also. In current years, we have seen extraordinary growth in the application of OSNs. For example, Facebook, one of ambassador social network sites, claims that it has more than 900 million active users and over 35 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each month. To protect user data, access control has become a central feature of OSNs. A typical Online Social Network provides each user with virtual space containing users profile information, a list of the user's friends, and web pages shared by online user, such as wall in Facebook, where users and friends can post content and leave messages for each other. In most of the developed social networks provide only the basic access control mechanism, e.g. a user can specify whether a piece of information shall be publicly available, private (no one can see it) or accessible only by direct contacts. The simple access control mechanism having advantage of being simple, intuitive and easy to implement. However, it is not good enough to fit with the requirements of all online social users.

Online social networks (OSNs) have attracted a large amount of users to regularly connect, interact and share information with each other for different purposes. Users share a tremendous amount of content with other users in OSNs using various services. The explosive growth of sensitive or private user data that are readily available in OSNs has raised an urgent expectation for effective access control that can protect these data from unauthorized users in online social networks (OSNs).

OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no power over data residing outside their spaces. Such as, if a user posts a comment in a friend's space, he/she cannot specify which users can view the comment. In another case, while a user uploads tags and the photograph friends who appear in the photograph, the tagged friends cannot restrict who can see this photograph, even though the tagged friends may have different privacy concerns about the photo. To address such a serious issue, beginning protection mechanisms have been offered by existing online social networks (OSNs).

OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their spaces. For example, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo, even though the tagged friends may have different privacy concerns about the photo. Because of this limitation we are developing collaborative management for shared data in OSNs, known as MPAC model.

It is believed that Social networks have challenges for mankind as well as its opportunities has a special dynamic attribute to human social development. To provide more evidence for this point, online social networks have both positive and negative sides, definitely, it is cheaper to use online social networking for both personal and business use because most of the services are free, and at the same time, users can easily develop their social life. However, for the negative side, sometimes users have to be extra-careful in using online social networks. This is because; there are many reporting cases of hacking of one's identity. Besides, this negative consequence, social networking sites (SNS) are online environments in which people create self-descriptive profiles and then make links with other people they know on the site.

II. RELATED WORK

Multiple user access control model is introduced for secure network access, existing access control solutions for online social networks trust based access control inspired by the developments of trust and reputation in online social networks. The friend of friend ontology based distributed identity management system for online social network where relationships are associated with a trust level which indicates the level of friendship between the users participating in a given relationship.

A. A Reachability Based Access Control Model for Online Social Networks

As a result of the widespread use of social networking sites, millions of individuals can today easily share personal and confidential information with an incredible amount of (possibly unknown), other users. This raises the need of giving users more control on the distribution of their resources, which may be accessed by a community far wider than they expected. Our concern is how to decide which users are allowed to see information owned by other users. Author's solution aims to support users when they wish to restrict the visibility of their resources to a smaller subset of their contacts. In this paper, author proposes a reachability based access control model that allows users to express their privacy preferences as constraints on existing links with other users. Experimental results verify the effectiveness of our approach over real social networks datasets. In this paper, Author developed an access control model for OSNs that enables a fine-grained description of privacy policies. These policies are specified in terms of constraints on the type, direction, depth of relationships and trust levels between users, as well as on the user's properties. This model relies on a reachability based approach, where a subject requesting to access an object must satisfy policies determined by the object owner.

B. A New Access Control Scheme for Facebook-style Social Networks

The popularity of online social networks makes the protection of users' private information an important but scientifically challenging problem. In the literature, relationship-based access control schemes have been proposed to address this problem. However, with the dynamic developments of social networks, we identify new access control requirements which cannot be fully captured by the current schemes.

In this paper, Author focus on public information in social networks and treat it as a new dimension which users can use to regulate access to their resources. Author defines a new social network model containing users and their relationships as well as public information. Based on the model, author introduces a variant of hybrid logic for formulating access control policies. In addition, author exploit a type of category relations among public information to further improve our logic for its usage in practice.

In this paper, author first identified a new type of access control policies that are meaningful but have never been addressed in the literature. Namely, users in social networks can express access control requirements not only based on their social relations, but also on their connections through public information. Then author defined a social network model containing users and public information. Based on this model, author proposed hybrid logic to define access control policies. Author gave a number of policies based on public information and formulated them precisely in our proposed logic. In addition, author has used category relations among public information to extend our logic and make it more practical. [1]

C. Relationship-based Access Control for Online Social Networks: Beyond User-to-User Relationships

In this paper, author develops a relationship-based access control model for OSNs that incorporates not only U2U relationships but also user-to-resource (U2R) and resource-to resource (R2R) relationships. Furthermore, while most access control proposals for OSNs only focus on controlling users normal usage activities, author's model also captures controls on user's administrative activities. Authorization policies are defined in terms of patterns of relationship paths on social graph and the hop count limits of these path. The proposed policy specification language features hop count skipping of resource related relationships, allowing more flexibility and expressive power. Author also provides simple specifications of conflict resolution policies to resolve possible

conflicts among authorization policies. [2]

In this paper, author developed an access control model for OSNs that provides finer-grained access control for user's usage and administrative access by utilizing user-to-user, user-to resource and resource-to-resource relationship-based policies. These policies are specified in terms of relationship path patterns between the accessing user and the target together with hop count limit of the relationships.

Specifically, author introduces the skipping of some relationship path expression in the policy specification in order to offer more expressive policies. The decision modules of the system determine authorizations by retrieving different policies from the accessing session, the target and the system, and then making a collective decision.

To address policy conflicts, authors apply conflict resolution policies over relationship precedence. In the future, author is planning to extend his model to incorporate attribute-based controls.

D. Identifying hidden social circles for advanced privacy configuration

With the dramatic increase of users on social network websites, the needs to assist users to manage their large number of contacts as well as providing privacy protection become more and more evident. Unfortunately, limited tools are available to address such needs and reduce user's workload on managing their social relationships.

To tackle this issue, author proposes an approach to facilitate online social network users to group their contacts into social circles with common interests. Further author leverage the social group practice to automate the privacy setting process for users who add new contacts or upload new data items. Author evaluates his approach using real-world data collected through a user study. Author also includes an analysis of the properties that are most critical for privacy related decisions.

In this paper, author proposed an approach which helps users in managing their social network contacts into relevant groups automatically, and also helps users set up their privacy policies automatically for their uploaded content. Organizing contacts into groups helps users set privacy settings for newly added content or new contacts joining their social circles.

E. A Privacy Preservation Model for Facebook-Style Social Network Systems

Recent years have seen unprecedented growth in the popularity of social network systems, with Facebook being an archetypical example. The access control paradigm behind the privacy preservation mechanism of Facebook is distinctly different from such existing access control paradigms as Discretionary Access Control, Role-Based Access Control, Capability Systems, and Trust Management Systems. Authors work takes a first step in deepening the understanding of this access control paradigm, by proposing an access control model that formalizes and generalizes the privacy preservation mechanism of Facebook. The model can be instantiated into a family of Facebook-style social network systems, each with a recognizably different access control mechanism, so that Facebook is but one instantiation of the model.

Author also demonstrate that the model can be instantiated to express policies that are not currently supported by Facebook but possess rich and natural social significance. This work thus delineates the design space of privacy preservation mechanisms for Facebook-style social network systems, and lays out a formal framework for policy analysis in these systems. Author formalized the distinct access control paradigm behind the Facebook privacy preservation mechanism into an access control model, which delineates the design space of protection mechanisms under this paradigm of access control. Author also demonstrated how the model can be instantiated to express access control policies that possess rich and natural social significance.

III. PROBLEM DEFINITION

To enable the protection of shared data associated with multiple users in OSNs with the help of access control mechanism.

IV. PRIVACY SETTINGS IN SOCIAL NETWORK

A. Facebook

Facebook's Privacy options are generally very flexible—so much so that you can get a little overwhelmed by them. Facebook's privacy settings are organized under five different categories, each with its own screen to go through and check. Though this seems like a lot, Facebook's privacy settings are actually considerably simpler than they have been in the past.

In an attempt to simplify matters some, the company offers up two different pre-configured privacy options that you can select from when you post something to your profile: "Public" and "Friends." As its name suggests, the "Public" option means that items you publish to your profile are visible to anyone who visits Facebook. Likewise, selecting "Friends" allows only your Facebook friends to see what you post. Facebook also offers a "Custom" setting: From there, you can pick and choose who gets to see what you post

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

by either restricting it to any networks you're part of or so that only people on selected "lists" (a way to organize your friends into groups--you can have a list for co-workers, for example, or for family) can see it. Additionally, you can also prevent specific people from seeing items you post. You can limit who can view your profile, whether it appears in search, whether others can tag you in photos or posts, and so forth.

Facebook's biggest strength in regard to its privacy settings is also its biggest weakness. The high degree of flexibility means you have relatively fine-grained control over who can see what on your profile, but the controls can still be rather confusing, even with recent attempts at simplification. It doesn't help that Facebook changes its privacy settings screens regularly, so you periodically may have to re-learn and re-adjust everything.

Following figure shows the different privacy setting available in facebook social network.

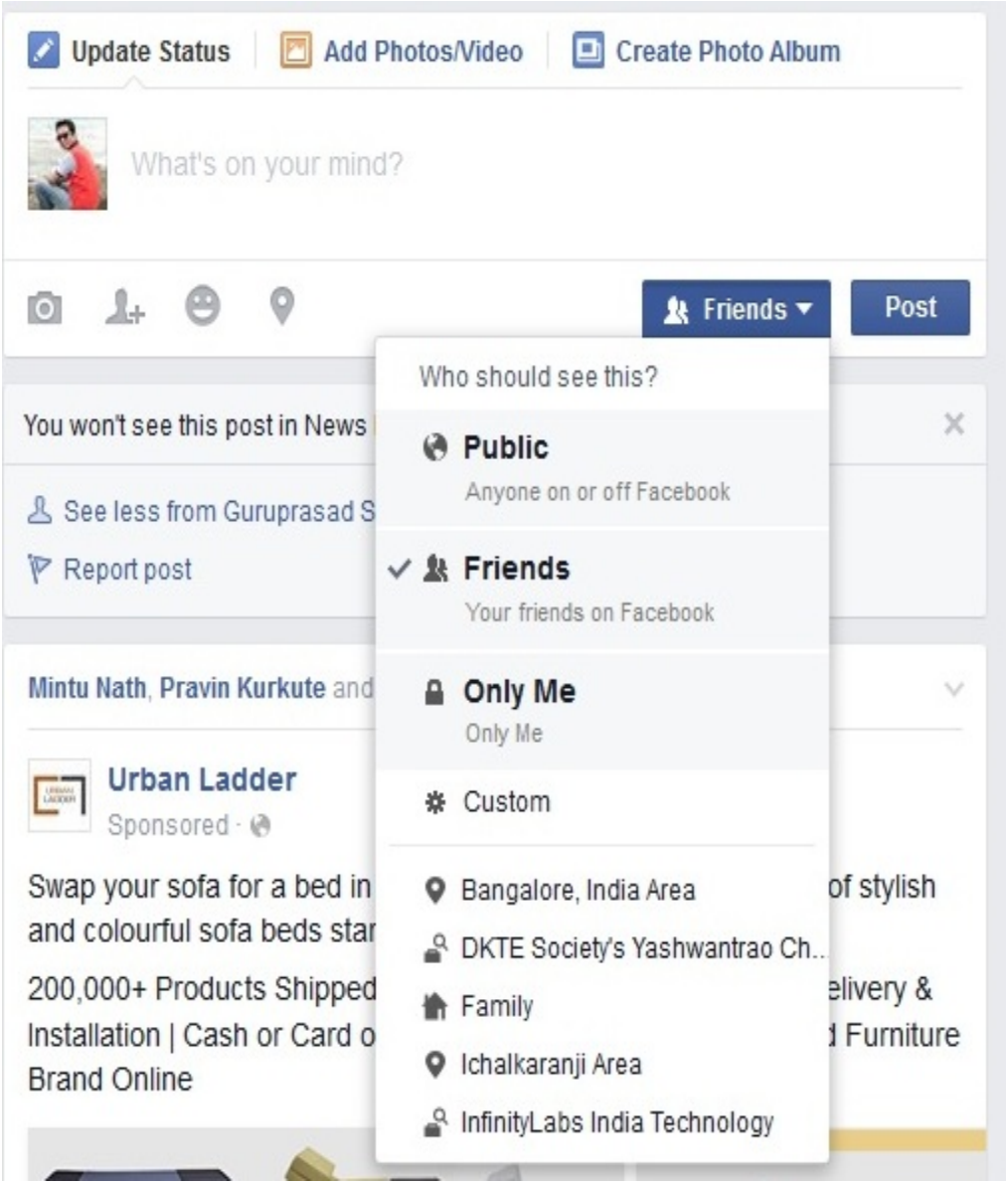


Figure: Privacy Settings Available In Facebook Social Network

V. ACKNOWLEDGMENT

First and foremost, I would like to thank Prof. Pingale S. V. for his most support and encouragement. He kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper. Finally, I sincerely thank to my parents, family, and friends, who provide the advice and financial support. The product of this review paper would not be possible without

all of them.

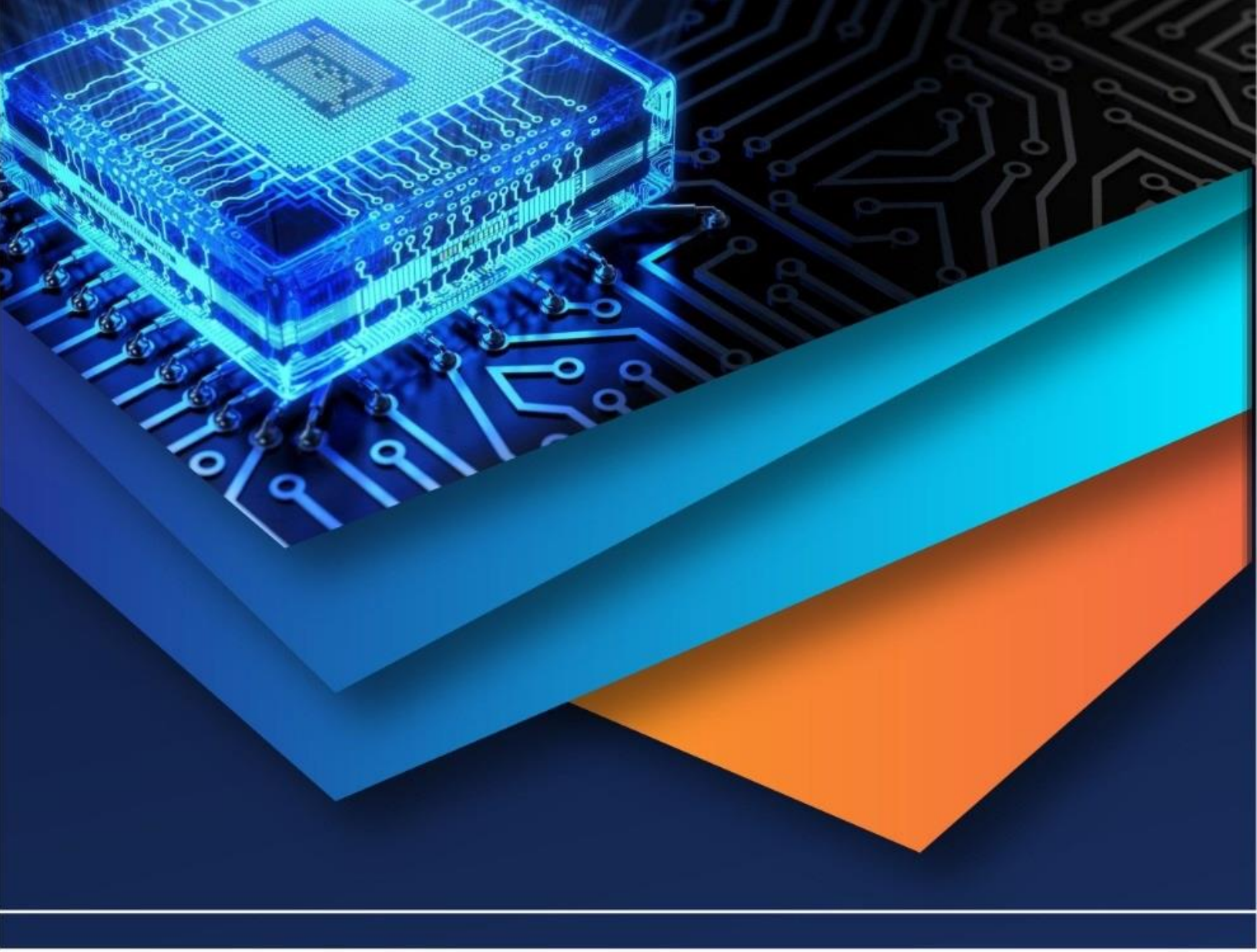
BIOGRAPHY

Prof. Subhash V. Pingale is the professor of the department of Computer science and engineering in SKN Sinhgad College of Engineering, Korti, and Pandharpur, India. His main areas of interest are Social Networks and web mining and their applications.

Mr. Sandip Shirgave was born in India, in 1988. He received the B.E. degree in Computer Science & Engineering from D.K.T.E College from Shivaji University, Ichalkaranji, India, in 2012, and pursuing the Master of Engineering degrees in Computer Science & Engineering from the SKN Sinhgad College of Engineering, Korti, and Pandharpur India. His main areas of interest are Social Networks and web mining and their Applications.

REFERENCES

[1] Pitkänen.O.Tuunainen, V.K, Hovi.M. 2009, Users' Awareness of Privacy on Online Social Networking sites – Case Facebook,https://domino.fov.unimb.si/proceedings.nsf/0/9b675b5e811394f0c125760000390664/$FILE/1_Tuunainen.pdf
[2] Zhang.Ch, Sun. J,Zhu. X, Fang.Y. 2010 Privacy and Security for Online Social Networks: Challenges and Opportunities. Univ. of Florida, Gainesville, FL, Chi USA
[3] Dwyer .C., Hiltz R., and Passerini K. 2007 "Trust and Privacy concern within social networking sites: A comparison of Facebook and MySpace", in the Proceedings of AM. Conference on IS .
[4] Goettke R. and Christiana J. Nov, 2007, "Privacy and Online Social Networking Websites".
[5] Govani, T., and Pashley, H. Nov 2007," Student Awareness of the Privacy Implications while Using Facebook" Unpublished manuscript retrieved.
[6] Gross, R.and Acquisti. 2005"Information Revelation and Privacy in Online Social Networks (The Facebook case)", in the Proceedings of the 2005 ACM workshop on Privacy in the electronic society.
[7] Quan-Haase, A. (2007). University students' local and distant social ties: Using and integrating modes of communication on campus. Information, Communication & Society.
[8] Exacttarget(n.d.) 58% of Consumers Begin the Day With Email http://pages.exacttarget.com/etlpgen?v=153
[9] J. Domingo-Ferrer, "A public-key protocol for social networks with private relationships," in MDAI, ser. Lecture Notes in Computer Science, V. Torra, Y. Narukawa, and Y. Yoshida, Eds., vol. 4617. Springer,2007, pp. 373–379.
[10] J. Domingo-Ferrer, A. Viejo, F. Seb´e, and ´U. Gonz´alez-Nicol´as, "Privacy homomorphisms for social networks with private relationships," Computer Networks, vol. 52, no. 15, pp. 3007–3016, 2008.
[11] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, G. Pelosi, and P. Samarati, "Preserving confidentiality of security policies in data outsourcing," in WPES, 2008, pp. 75–84.
[12] K. B. Frikken and P. Srinnivas, "Key allocation schemes for private social networks," in Proceedings of the 8th ACM workshop on Privacy in the electronic society, 2009, pp. 11–20.
[13] B. Carminati, E. Ferrari, and A. Perego, "Rule-based access control for social networks," in OTM Workshops(2), ser. Lecture Notes in Computer Science, R. Meersman, Z. Tari, and P. Herrero, Eds., vol. 4278. Springer, 2006, pp. 1734–1744.
[14] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attributebased encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY