iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** X **Month of publication:** October 2015

DOI:

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Access Control Model For Online Social Networks

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

Abstract— This We have seen the widespread use of online social networking sites, there are hundreds of millions users can easily share private and public information with online unknown users. For this reason it is important to give more access on shared data. Our aim is to decide which online users can see information authorized by owner of the information. Our solution aims to provide users when they wish to avoid or restrict to see of their information to their friend list. In this paper we see the reachability control model that allows user can set their privacy concerns with existing online users.
Keywords— Security, integrity, and protection, Access Control, Online Social Networks

I. INTRODUCTION

With the fast development of web 2.0 technologies in last five years, social networks such as orkut, linked-in, twitter, facebook, YouTube and flicker etc. are become the most successful we services on the web. These types of Online Social Networks offer digital social interactions and information sharing, but also raise a number of security and privacy issues on data which is shared in social networking space. Facebook now claims that it having over 500 million active users and Twitter has 200 million users. Facebook, one of representative social network sites, claims that it has more than 800 million active users and over 30 billion pieces of content such as web links, news stories, blog posts, notes, photo albums shared each month. The availability of this information creates privacy and confidentiality issues over data which is shared in online social network. Online social users typically do not want to share all of their information with everyone. 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.
It is either too loose because it grants access to all online social users (public), or it is too restrictive by limiting too much information sharing (private). Such simple access control strategies have the advantage of being straightforward, but, on one hand, they may grant access to non-authorized users, and, on the other hand, they are not flexible enough in denoting authorized users. Although Online Social Networks currently provide simple access control mechanisms allowing users to control access to information contained in their own spaces, users, unfortunately, have no control over data residing outside their virtual online spaces. For instance, if a user posts a comment in a friend's space, she/he cannot specify which users can view the comment. Based on such considerations, we will conclude the different types of access control methods available today.

II. PRIVACY

Privacy is the right or opportunity to decide who has access to your personal information and how that information should be used. The issue of privacy within social networking sites are still uncleared. It means user or individuals can control the information which is visible to others not. More than a few studies have attempted to determine implications of privacy concerns and awareness of privacy to users' online practices and behaviour. In any online social network users are generating a large amount of data. Protecting online users from other online users includes any other user on the social network. We can divide the set of other users into three categories.

A. Directly Connected Users

These are users that have a link between them in the social graph. This means something different in different social networks. In

©IJRASET 2015: All Rights are Reserved

Facebook it means that the two users can view more information on each other's profiles. In some of the literature this simply means the two users have communicated with each other via email. Many online social network providers like facebook, twitter allows the users of their social network to make privacy settings. This is the user's first line of defence against malicious users. Some of these privacy setting schemes are simple and straightforward. For example, Twitter allows users to make tweets private which are only visible to their followers. These privacy settings must be carefully weighed and experimented with, and yet users are forced to make privacy settings immediately upon joining the social network in order for them to be successful in protecting their own data.

B. Indirectly Connected Users

These users are two or more hops away from one another. (e.g., friends of friends (FOF) or friends of friends of friends (FOFOF)). This category also includes two users that are in the online social network that have absolutely no relation between them. It means between two online users no relation present between them. One of the more subtle issues in protecting user data from other users is the spread of sensitive, partially private content. The key difference between this and the previous section is malicious users accessing other user content directly vs. indirectly. A malicious user accesses information indirectly when some third party user spreads that information. Social networks typically try to define some set of rules for the online user to define who can view their information and who cannot. Anybody, however, is allowed to publish information.The main problem with these online social networking sites is that users that have access to the sensitive, hidden data of another online user can simply use their ability to publish to spread that data to online users whom are not supposed to have access to it or not supposed to can see it.

C. General Public

The general public has access to information in many online social networks. For example, Twitter makes tweets public by default and Google indexes them.

III.THE SOCIAL NETWORK MODEL

As shown in following figure, a online social network is a dynamic structure made of nodes, which are connected to each other through various relations as shown in figure. The nodes and the edges shown in the graph/figure represents, the online social network users and the relationships present between them. Labels shows the relationship type associated to each edge, i.e., Alice considers Bill her friend, Colin considers David his friend, and so on. In this framework, relationships are not similar, i.e., if Alice considers that Bill is her friend, it doesn't mean that Bill considers Alice a friend too.

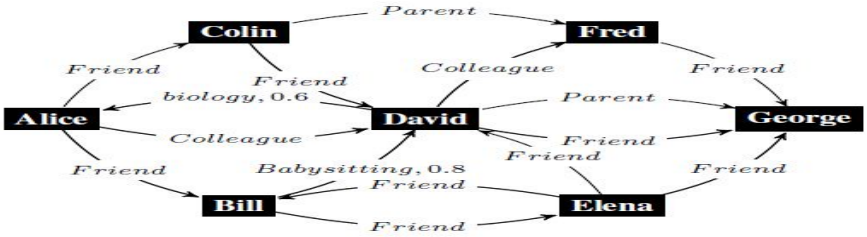


Figure 1: - The Social Network Model

IV. THE ACCESS CONTROL PROTOCOL

An access control model implies the specification of both the access control policy and the access control enforcement mechanism, which represent, respectively, the desired rules according to the high level requirements of the system and the implementation of this policy.

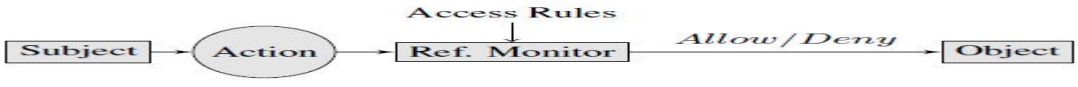


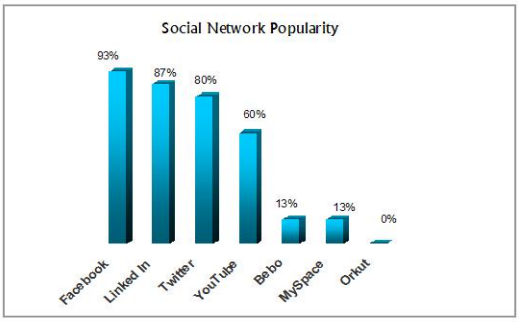
Figure 2:- The Access Control Protocol

©IJRASET 2015: All Rights are Reserved

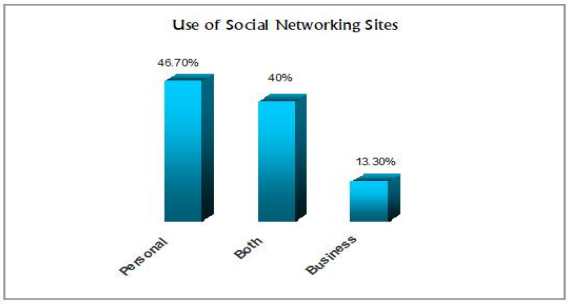
Volume 3 Issue X, October 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

As shown in above Figure 2, the fundamental components of our access control model are:
The Subject, also called Principal, is a person who tries to get access to a particular resource, i.e., the object.
The Action is the operation that the subject wants to execute over the object.
The Object is the target resource, to which access may need to be controlled.
The Reference Monitor is the component that implements users privacy preferences, i.e., access control policies. It takes as input a set of access rules according to which it will allow or deny access to a given object or resource. The access control enforcement mechanism is performed by the reference monitor, which is a trusted software module that intercepts each access request submitted by a subject to access an object and, on the basis of the specified access policy, determines whether access should be granted or denied to the requestor.

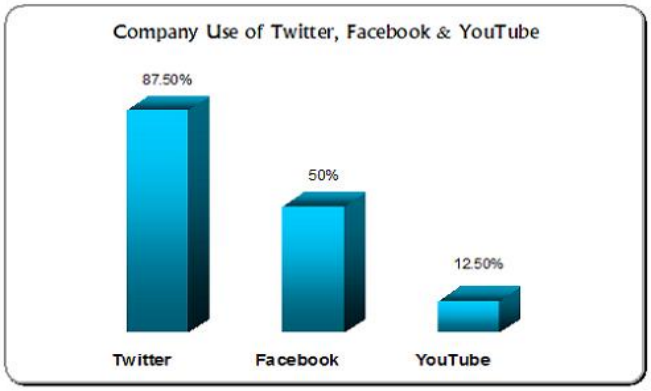
V. SOCIAL NETWORK POPULARITY



VI. USE OF SOCIAL NETWORKING SITES



VII. COMPANY USE OF TWITTER, FACEBOOK & YOUTUBE



©IJRASET 2015: All Rights are Reserved

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

VIII. ADVANTAGE AND DIS-ADVANTAGE

	Advantage	Disadvantage
1	Worldwide Connectivity	Face to Face Connections are endangered
2	Commonality of Interest	Cyber-bullying and Crimes against Children
3	Real-Time Information Sharing	Risks of Fraud or Identity Theft
4	Free Advertising	Time Waster
5	Increased News Cycle Speed	Corporate Invasion of Privacy

IX. CONCLUSION

In this paper we have seen advantage and disadvantage of social networking sites and also usage of social networking site company usage of different social networking sites and different social networking sites with their popularity. We also discussed access control protocol and we also seen the social networking model.

X. 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



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.

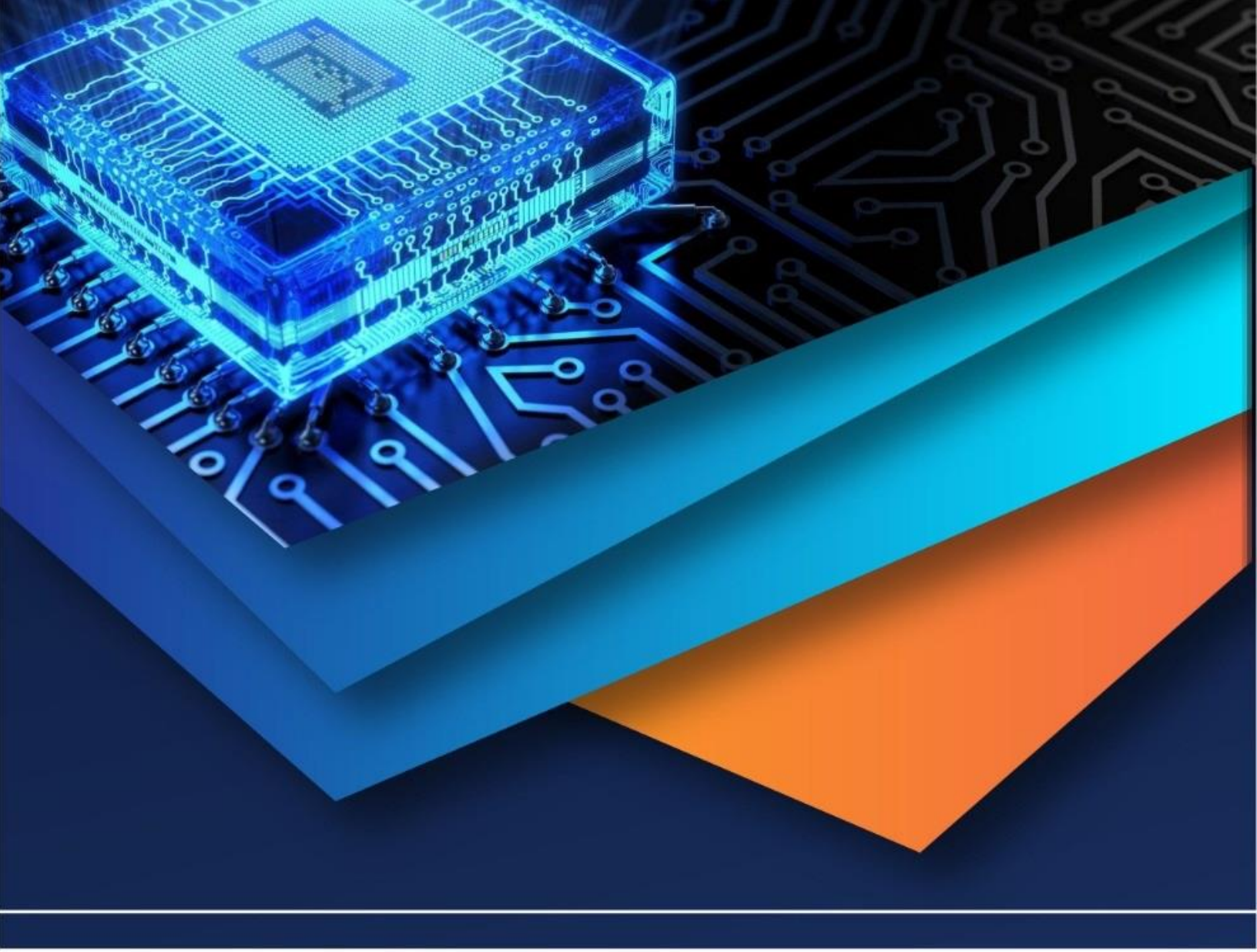
Prof. Subhash V. Pingale is the professor of the department of Computer science and engineering in SKN Sinhgad College of Engineering, Korti, and Pandharpur, India. His main areas of interest are Social Networks and web mining and their applications.

©IJRASET 2015: All Rights are Reserved

REFERENCES

[1] Carminati, B., Ferrari, E.: Enforcing relationships privacy through collaborative access control in web-based social networks. In: Proc. 5th International Conference on Collaborative Computing (CollaborateCom), IEEE CS (2009) 1-8.
[2] S. Kruk, S. Grzonkowski, A. Gzella, T.Woroniecki, and H. Choi.D-FOAF: Distributed identity management with access rights delegation". The Se- mantic WebASWC 2006, pages 140154, 2006
[3] 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 17341744. Springer, 2006
[4] P. Fong, M. Anwar, and Z. Zhao. A privacy preservation model for facebookstyle social network systems. In Pro-ceedings of the 14th Euro- pean conference on Research in computer security, pages 303320. Springer- Verlag, 2009.
[5] E. Carrie. Access Control Requirements forWeb 2.0 Security and Privacy. In Proc. of Workshop on Web 2.0 Security and Privacy (W2SP). Citeseer, 2007.
[6] F. Paci. Collective privacy management in social networks. In Proceedings of the 18th international conference on World wide web, pages 521530. ACM,2009.
[7] http://socialnetworking.lovetoknow.com/Advantages_and_Disadvantages_of_Social_Networking
[8] http://www.livlarge.co.nz/tag/social-networks/

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)