ISSN: 2320-1363

Prevent the data loss using hybrid collaborative filtering recommendation model in social network websites

Kadham V. Sudeep kumar*1, K.MohanaRao*2

M.Tech (CSE) Student, Department of CSE, PEC, Kandukur, Dist: Prakasam, AP, India

Associate Professor, Department of CSE, PEC, Kandukur, Dist: Prakasam, AP, India

Abstract:

The Social Networking Web Sites (SNWS) like Face book, Google, Twitter, etc.., may provide third party applications. These third-party apps may consist of gaming and productive application platform in order to draw user attention. These social networking sites consist of millions of users accessing billions of third-party apps and their activities are in increasing manner from day to day. It consist exposure of user's sensitive and confidential data to the third-party vendors. Although, the existing system O Auth provides Open Authentication Standard Protocol access for efficient security issues. But it doesn't provide any recommendations towards user in order to reconfigure the third-party apps. Here it doesn't consists of fine-grained approach due to this the user is in dilemma state and over helmed by third parties.

In this paper we discuss the enhanced issues of OAuth, OAuth2 that is Proposed OAuth2.0 (or) Multi-Criteria based Recommendation model. This model is mainly based on collaborative filtering and prediction model. The collaborative filtering is sub categorized into user based, category based and application based categories, here the user considers and entemplates about previous users decisions, through this predictions and various recommendations in browser's extensions. These Recommendations acts permission guide for users, it is an efficient way for selection and provides awareness on various third-party application authorizations.

Keywords: Social Networking Web Sites, O Auth, collaborative filtering, Multi criteria based Recommendation model.

I. Introduction:

The Social Networking Web Sites (SNWS) are concerned as hub for billions of third-party applications in the modern society. These third-party applications, within Social Networking Sites (SNWS) have become very familiar and penetrative. Due to this drastic increase of third-party

ISSN: 2320-1363

apps they may have possibility to access user's information in social networks such as fb (or) twitter.

The user have initiation of using any application besides that users are required to authorize them and allow them to access certain permissions of their basic information such as user name, dob, e-mail, locality, etc. There is no idea how to prevent them? Permissively through with our one time allow permission they share user's online public or private data has its necessity. The third-party vendors and open standards had contributions to provide specific internet user tools to maintain their privacy and confidential issues and these are seen by World Wide Web Consortium/Firm (W3C) to build the Platform for Privacy Preferences (P3P) and Preference Exchange Language (APPEL) most of the websites use this machine readable format in particular privacy policies .

Definition of OAUth: The OAuth is a protocol for developing password less Application Programming Interfaces (APIs).It acts a way for an application to interact with an API on a user's behalf without knowing the user's authentication credentials with some permitted issues.

Third-party application vendors have led charges to improve user privacy through enhancing extensions' in the web browsers such as safari fire fox and Google. These extensions in browsers aware the user from irrelevant advertisements and unauthorized software installations and vow's the user credential data. While Joshi's IMSAA explains a browser plug-in in which attempts to form a solution man-in-middle attacks prevalent in now a day's phishing attacks. There is a partner-ship between browser's extension and open standards is very high in history and likely to prolong, but there may be a small gap that needs fulfilling. The concept of individual privacy may be just an individual; it is an appreciating concept that an individual privacy preferences are just single through an individual extension that request the privacy suspects for a unique set of individuals. So, that's why we propose a novel extension of FBSecure has been implemented in this paper, a proposed recommendations model entemplates about users to make permissive privacy decisions at the time of third-party installations and integrates in the present existing system.

The browser's extension's act's as simple interface, a multi-criteria recommendations are provided through collaborative effort. It consists of pervious user's historical data and may be helpful for user to select appropriate permissions towards the third-party apps on their own in the social networking sites.

II. Problem of Existing System:

ISSN: 2320-1363

The O Auth provides a technique for third party vendors to access users resources without allowing the users credentials to the vendor's. But it doesn't provide any recommendations towards user to make appropriate decisions. For example we use through-out this paper is one of the free Face book online video and voice calling applications available through friendcameo.com. The Friend Cameo Face book application requests the following extended permissions when a user first installs the application: access to the user's e-mail address, ability to publish status and post messages to the user's wall, the ability to access the Face book chat application, and the ability to enumerate the online presence status of other users. We make no value judgment of the extended permissions requested by the example applications presented in this paper. The friend cameo is a face book applicant, follows extended permissions to install an application: by accessing the user's e-mail, ability to post the messages and status in the user's wall. It has the ability to access the face book chat application of user in presence of other user's status. It aware's user quickly that some of the extended permissions can't be revoked genuinely. So there aspects can overcome in the proposed system.

III. Related work

The existing approach relationship based on access control policies, this Relationship related to information is called as role based access control and coalition based access control. Here Each and every user enters the role based information. The user verifies the data and releases information to various users. Sometimes same user has a chance to present the multiple relationships environment that's why Conflict problem may raise here. This type of approach provides the limited dimensions of security and privacy mechanism result. It is not efficient approach.

The other access control technique is fine grained approach. Here, we have to consider a small example that consists of content as blog article information, photos and personal information. It initiates, initial permission information may release the normal data. After completion of initial step directly it is not possible to show the whole data. In a blog article some of the words of content we maintain as a securable data. In total number of users which users have next levels of permissions those users its possible access the important words information. Two levels of fine grained format also it is not to control the attackers and it may leads to access the user's content of information. Hence this type of access control technique is not efficient.

ISSN: 2320-1363

Another access control technique is firewalls. It filters based on IP addresses, port numbers, and protocol types. These properties are insufficient for detection of all attackers. Some of the attackers are entering from remote locations, those users information is not possible to detect with the help of firewall environment. Instead of firewall policies it may have chance to control the attackers in detection environment.

The Browsers are implementing the third party applications code environment. They are mainly focusing to increases the privacy environment constraints settings information. Initially we have to check the present third party application code behavior and identify the problems. Now, consider the identified problems and enhance the third party application code information. In a new browser configuration setting we add the code into three locations. They are content scripts, core extensions and plug-ins environment. These new properties some new attackers it may chance to inject here in implementation process.

The access control technique is based on attribute based access control scheme. In this technique, we are going to add some additional features related to cryptographic environment. After it satisfies the first attribute information data owner may publish or release the data environment. It is also controlling the original data of content environment specification process.

The above related work templates about some limitations of content information in implementation.

IV. Contributions

a. The browser extensions may provide identity attributes in order to verify user credentials through a simple interface.

b. A simple interface makes the decisions for protection before installation of third-party app.

c. The collaborative model provides multi dimensions to obtain various decisions. In all collaborations identifies the similar requested privacy options, these similar requested privacy options we consider as a recommendations.

d. Recommendation based privacy attributes helps us to make important decisions. These Recommendations are concerned as a good assistance for user decision making.

e. After observation all third party applications recommendations, which third party application have more number of recommendations that application we install here for better privacy and security.

f. It gives the enhanced security and privacy results.

ISSN: 2320-1363

V. Proposed System Architecture

The proposed system is an efficient and secured technique for authorizing third-party application. It requires various users to present their credentials towards third-party applications; hence they allow huge access to all their resources without any restrictions. Here we enhance O Auth with new credentials are allowed by using Access Token. Access Token is a string that denotes to certain scope of permissions allowed to a third-party application and it also signifies the other attributes like duration of access token, here we showed interest on scope of character within the access token, that was issued by an Authorized server through allow permission granted by user. Here we used an abstract access paradigm that is used to design filtering systems.

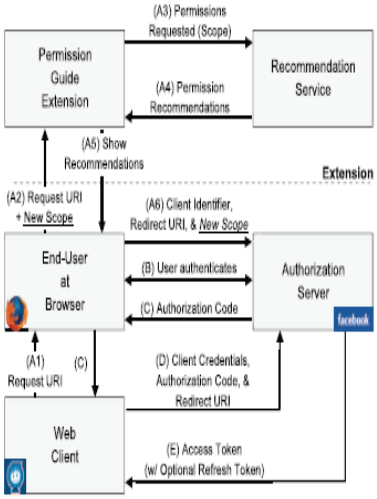


Fig.2: Proposed System Architecture of O Auth & User Privacy.

VI. Proposed O Auth flow:

The enhancement of Oauth2.0 consists of Recommendations and Permission Guide.

6.1 Recommendations: It gives a set of recommendations for the requested permissions by using collaborative filtering as seen section 4. **Permission Guide:** It guides the users through the requested permissions and gives them a set of recommendations on each of the requested permissions. Detailed explanation of permission guide is given in section

A1. The user/web client redirects the browser to the end-user authorizing at end point by initiating a request through URI, which includes a Scope parameters.

A2. The Permission Guide extension catches the scope values from the requested URI, then parses the requested permissions.

A3. The permission guide extension, requests a set of recommendations on the parsed permissions. These are achieved by passing the set of permissions to our Recommendation Service.

A4.The Recommendation Service provides a set of recommendations towards the permissions requested by the user.

A5. By using a set of obtained recommendations these extensions may provides the permissions with their

ISSN: 2320-1363

recommendations are in user-friendly manner.

A6. The Permission Guide redirects the end user's browser to a new URI, which consists of new scope parameters. By assuming the user chooses to modify the requested permissions.

6.2 Permission guide Description:

The Permission Guide is an extension of browser that combines the authorization process by accessing the scope parameter values within the requested URI created by a third-party application. If the scope is accessed, the extension may parses the requested permissions are provided in user-friendly manner.

Initially we have to look over the recommendation which was released by user releasing permissions. Based on those recommendations, we can predict the values through grant (or) deny operations. If grant permission is given there is no data loss. Checking / un checking permissions are done through recommendations. A formal considers a face book chat list it shows a Face book-chat rather than xmpp-login. This type of extension shows the users a set of recommendations for the requested permissions. For each and every permission there should likes and dislikes they are certain recommendation values. These recommendations are predicted through certain prediction values, they are calculated and shown in the concept of recommendation models, these predicted values are represented as grant (or) deny permissions. The user may perform grant (or) deny permissions which is based on previous decisions made by collaborative decisions of other users. We can customize the requested permissions by check/uncheck permissions. If checked it is represented as '1' then user wishes allow the third-party application are else vice-versa ('0' to deny the permissions) that's why we used Set permissions button as an extension. This extension is used to create a new request URI with a new scope Scope1 and it forwards the user browser as new request URI. Here it is classified as scope1 sub set and equals to scope. An example of Scope1 for Friend Cameo application as follows:

Scope1=publish_stream

It shows impact on user's decision to allow Friend Cameo the feed, but restrict to access e-mail, Face book chat list. Here by using subset of permissions requested could potentially delay the functionality of third-party app once it gets installed. By interrogating such consequence is out of scope in this paper, but we include this part of our future work. Permission Guide extension also collects the user's decisions on the requested permissions, hence it allows us to generate a data set of decisions to be used in our recommendation model explained through O Auth and privacy i.e., our Recommendation Service as seen in Fig.

ISSN: 2320-1363

2 will utilize these decisions in making its recommendation predictions. Those decisions are uploaded to servers once a user sets her desired permissions within the extension, and then clicks the Set Permissions button. The data uploaded to our servers includes: app_id, requested_parms, decisions, recommendations, the app_id is the application's primary id which is assigned by the service provider (e.g: Face book), the requested parameters is the scope of permissions requested by the third-party application, these decisions are the individual user decisions (grant or deny) on each of the requested permissions, and the recommendations are the recommendation values at the time the user made their decisions.

Our main motto is to provide a user-friendly interface for interactions with these permission requests, hence increasing user awareness and providing a simple mechanism for guiding users in making their decisions. The users through the requested permissions and gives them a set of recommendations on each and every requested permissions.

6.3 Modules:

The proposed system architecture implementation divides as a number of modules. They are:

1. Open authentication and privacy
2. Collaborative mechanism
3. Recommendation model
4. Prediction model

Open Authentication and privacy:

An open authentication standard installs the third party applications. These third party applications are categorized based on role wise. Role based users environment approach increase the privacy. Any user forward the request related to privacy attributes automatically third party service provider show the access tokens information. These access tokens are show the grant or deny permissions information.

Collaborative Mechanism:

After completion of authorization next authentication server provide URI with permission list. Permission list is called scope parameters. Scope parameters list is parse based on permission guide extension procedure. Parsing gives the subset of permissions list only. Subset of selection permissions also works based on recommendation model service.

D:ApplicationsXUsers.→eq1
D=d1, x d2…d (n-1), x d (n).

Consider an example from the above Fig.3 with elements as follows:

ISSN: 2320-1363

D=Finaldecision,
A=Applications,
U=Users.

In this model uses a set of permissions (P) as asset of criteria, then each permission 'pj' belongs to P. consider an example let p1= birthday, p2=e-mail, and p3=location similarly ,u1= Apple u2= Boss and a1, a2, a3 are various Applications. Where each represents a single criteria within a 3 dimensional model. Here u1= Apple is a user , install an application a1 as grant which is represented as d1='1' , d2='0' as deny permission and d3='1' as grant permission. A single decision has to be taken on each permission and it is represented in a multi-dimensional matrices model. The value representation as follows: 1= grant. 0=deny. ?=dilemma (or) yet to make decision. From the above decisions made by users on various applications and their permissions are plotted into a matrix format as Ga=(a1,a2,…an),permissions (birthday, e-mail, location) and their correspondence as shown as Ga(j,k) values.

Recommendation Model:

Recommendation service provides the set of recommendations information for each and every permission. Recommendations are calculates based on user access requests. Whenever numbers of requests are increases new scope is generate here. Automatically numbers of choosing permissions are increase manner. The recommendation service extends upon permission guide extension. Consider A, U, P as Applications, User, and Permissions from the above Fig.3 illustrates about the permission as detailed explained in collaboration model.

Prediction Model:

This model is based on calculations of various predicted values based on previous user's decision and gathers new user's decisions information. These prediction values are identified and based on collaborative filtering.

I. Modules in Brief

A. **Web-client/user:** In order to access his/her account and third-party application, the user needs login to his/her account through user name and password. Else the user doesn't register yet he/she has create new account with their basic information. This data provided by user will be stored in server database for future usage.

B. **Browser:** It acts as a mediator between User, permission Guide, and Authentication Server.

- It accepts req from client & forwards to Permission Guide.
- It receives recommendations from Permission Guide.

ISSN: 2320-1363

- It redirects URI and Authorization code forwards to user from server.

C. **Permission Guide:** After successful registration by user to server. If the user wants to access the access the third-party app then permission guide extension requests the scope and retrieves the recommendations.

D. **Recommendation Service :** it provides various recommendations

E. **Authentication Server:** The server redirects URI requested by the user from browser, then the user authenticates an authorization code from Authentication Server to user via browser. After that server redirects URI and credentials from user, then server allows an Access Token towards user.

II. Implementation Part:

In this paper we design the face book application. It we create with the help of JSP pages environment. All users registration information store in admin.In administrator side only access register the new third party application with different permissions list content. Next after that in user side normal access permission list is available without any recommendations. Next Proposed open authentication shows the all permission list. Now first choose the subset permission list information. Next all permissions list show the recommendation results information also. User it may chance to take the good decision in choosing permission list. Third party service providers show the access tokens information. In administrator side show the results of increased recommendations information. In administrator side we show the collaborative filtering matrix.

VII. Output Screens:

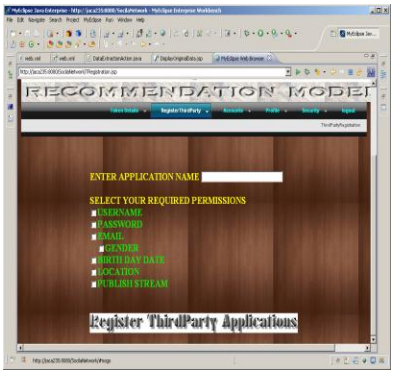


Fig4: New third party application Registration

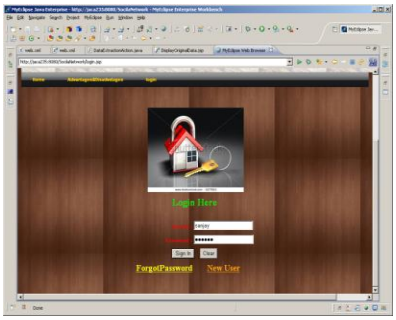


Fig5: Login page

ISSN: 2320-1363

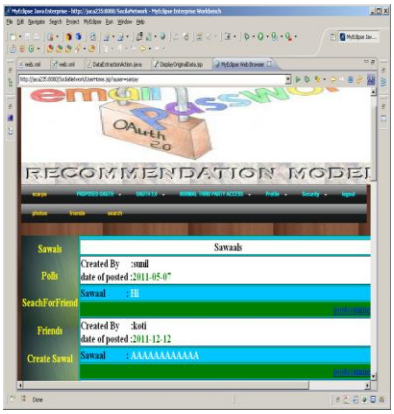


Fig 6: user home page information

Fig 7: Choose the third party application

Fig8: Display the permission list information for normal access

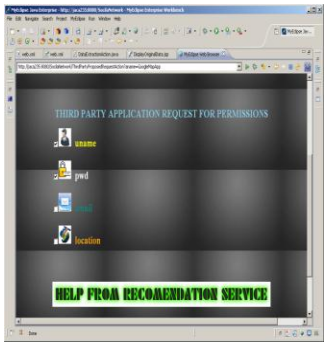


Fig9: proposed system related permission list

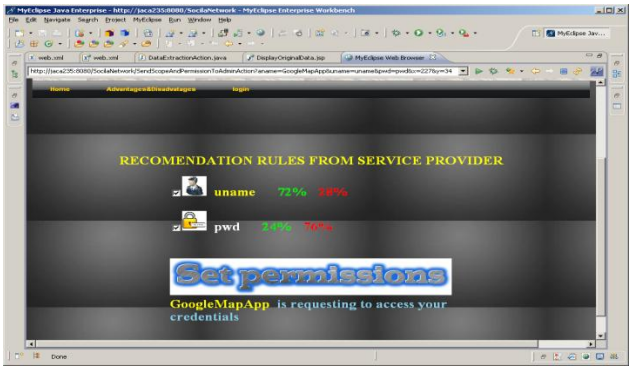
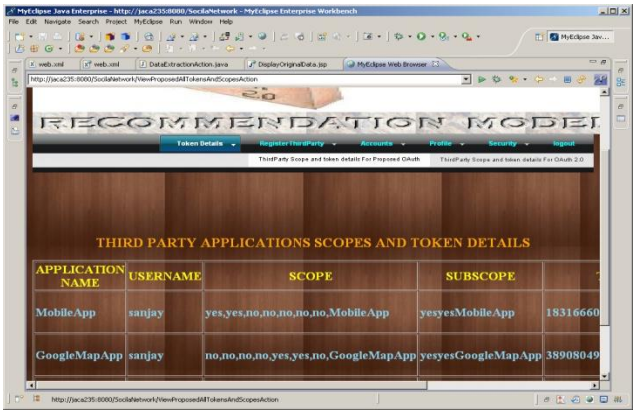


Fig10: Display the recommendation information



ISSN: 2320-1363

Fig11:Display the access tokens information

VIII. Conclusion & Future work:

Third party Configuration tools provide the good user protection and privacy on private data. The existing system related third-party application permission list user make decisions is not appropriate. It may have chance to loss of data. Now in this implementation we show the browser configuration extension process with recommendation service. These Recommendations we calculate based on multicriteria model. All users similar requests information define as a recommendation. Consider the recommendation user make the important decision and save the original data of content information. If no of recommendations are increases and user gives the new permissions information content. In the future, we will work on an address possible application mis configurations due to insufficient permissions and application permission evolution over time. We also plan on investigating hybrid and probabilistic collaborative filtering systems for providing better predictions in cases of parse user decision data. we would like to investigate the merits of our approach on other platforms, e.g., mobile platforms. Additionally, We also like to investigate the benefits of providing additional information (e.g., population age distribution) to users when making their privacy decisions.

REFERENCES:

[1] A. Acquisti and R. Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," Proc. Int'lWorkshop Privacy Enhancing Technologies, pp. 36-58, 2006.

[2] G. Adomavicius and Y. Kwon, "Multi-Criteria Recommender Systems," Recommender Systems Handbook: A Complete Guide for Research Scientists and Practitioners, Springer, 2010.

[3] G.-J. Ahn, M. Ko, and M. Shehab, "Privacy-Enhanced User-Centric Identity Management," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 1-5,2009.

[4] A. Besmer, J. Watson, and H.R. Lipford, "The Impact of Social Navigation on Privacy Policy Configuration," Proc. Sixth Symp.Usable Privacy and Security (SOUPS '10), July 2010.

[5] W. Bin, H.H. Yuan, L.X. Xi, and X.J. Min, "Open Identity Management Framework for Saas Ecosystem," Proc. IEEE Int'l Conf. e-Business Eng. (ICEBE '09), pp. 512- 517, 2009.

[6] D. Carrie and E. Gates, "Access Control Requirements for Web 2.0 Security and Privacy," Proc. Workshop Web 2.0 Security & Privacy(W2SP '07), 2007.

[7] S. Chen and M.-A. Williams, "Towards a ComprehensiveRequirements Architecture for Privacy-Aware Social Recommender Systems," APCCM '10: Proc. Seventh Asia-Pacific Conf. Conceptual Modelling, pp. 33-42, 2010.

[8] Facebook, Facebook Press Room, http://www.facebook.com/press/info.php?statistics, 2011.

[9] L. Fang and K. LeFevre, "Privacy Wizards for Social Networking Sites," Proc. Int'l Conf. World Wide Web (WWW), M. Rappa, P. Jones, J.

ISSN: 2320-1363

Freire, and S. Chakrabarti, ed., pp. 351-360, 2010.

[10] A. Felt and D. Evans, "Privacy Protection for Social Networking Platforms," Proc. Workshop Web 2.0 Security and Privacy, 2008.

[11] A.P. Felt, K. Greenwood, and D. Wagner, "The Effectiveness of Application Permissions," Proc. Second USENIX Conf. Web Application Development (WebApps '11), p. 7, 2011.

[12] FriendCameo, Inc., FriendCameo, http://friendcameo.com, 2010.

[13] J. Goecks, W.K. Edwards, and E.D. Mynatt, "Challenges in Supporting End-User Privacy and Security Management with Social Navigation," Proc. Fifth Symp. Usable Privacy and Security (SOUPS '09), pp. 5:1-5:12, 2009.

[14] D. Goldberg, D. Nichols, B.M. Oki, and D. Terry, "Using Collaborative Filtering toWeave an Information Tapestry," Comm. ACM, vol. 35, no. 12, pp. 61-70, 1992.

[15] K.K. Gollu, S. Saroiu, and A. Wolman, "A Social Networking-Based Access Control Scheme for Personal Content," Proc. 21st ACM Symp. Operating Systems Principles (SOSP '07), 2007.

[16] R. Gross and A. Acquisti, "Information Revelation and Privacy in Online Social Networks," Proc. ACM Workshop Privacy in the Electronic Soc. (WPES '05), pp. 71-80, 2005.

[17] M. Hart, R. Johnson, and A. Stent, "More Content - Less Control: Access Control in the Web 2.0," Proc. IEEE Web 2.0 Security & Privacy Workshop, 2003.

[18] J.L. Herlocker, J.A. Konstan, A. Borchers, and J. Riedl, "An Algorithmic Framework for Performing Collaborative Filtering," Proc. Int'l ACM SIGIR Conf. (SIGIR '99), pp. 230-237, 1999.

[19] J.L. Herlocker, J.A. Konstan, L.G. Terveen, and J.T. Riedl, "Evaluating Collaborative Filtering Recommender Systems," ACM Trans. Information Systems, vol. 22, pp. 5-53, Jan. 2004.

[20] A. Herzog and N. Shahmehri, "User Help Techniques for Usable Security," Proc. Symp. Computer Human Interaction for the Management of Information Technology (CHIMIT '07), 2007.

[21] M. Jenkin and P. Dymond, "A Plugin-Based Privacy Scheme for World-Wide Web File Distribution," Proc. 31st Hawaii Int'l Conf. System Sciences, vol. 7, pp. 621-627, Jan. 1998.

[22] Y. Joshi, D. Das, and S. Saha, "Mitigating Man in the Middle Attack over Secure Sockets Layer," Proc. IEEE Int'l Conf. Internet Multimedia Services Architecture and Applications (IMSAA), pp. 1-5, Dec. 2009.

About the Authors:

1.) Mr. **Kadham V Sudeep kumar** pursuing M.Tech [CSE] from Prakasam Engineering College, Kandukur, Andhra Pradesh.

E-mail Id:kadhamsudeep@gmail.com

ISSN: 2320-1363

2.) Mr. **K.Mohana Rao** Working as Associate Professor in Department of Computer Science & Engineering in Prakasam Engineering College, Kandukur, Andhra Pradesh.
My interested subjects are Computer Networks, OOAD,DS.....

E-mail Id: mohanakalavakuri@gmail.c