Secrecy Regulation and Obstruction of Photo Theft on Social Platform

I. Mary Linda, C. Anuradha, S. Pothumani

Abstract*: Nowadays, People are well-connected to one another in Social Networks. Usage of Internet and involvement in Online Social Platforms are increasing day by day. People sharing their personal information in these platforms. Even, they started Uploading their Photo in the Internet and it became very common among the Internet users. Without understanding the risk, user involved in sharing their personal details. Some fraudulent users uploading another user's photo without their knowledge. They are getting photos of others in many ways such as by taking photos using their mobile cameras, collecting images from Social networks, stealing images from the theft mobile. They are posting the photos in the Social media applications which are stored enduringly in the database. This results in the misuse of photo and involved in many criminal activities. To overcome this security problem, a competent face recognition system is needed which identify the user in the photo. To handle this, a set of users, friends list and their private photographs. This system accomplished as an evidence of approach in social network on Facebook application.

***Index Terms*—Photo Theft, Internet Platform, Collaborative approach, Securing Image**

I. INTRODUCTION

Internet has become very popular and the usage of Internet applications increased rapidly. People started using Online Social application such as Facebook and spend their time in the Social sites. It becomes an imperative part in their day to day life. People likes to involve in these Social
sites to share the information with one another. The way of interaction between the people and the communication process have been changed nowadays. They started to connect in Social sites and providing the details about themselves without understanding the risk. User create an account in the Social sites by providing all their important details such as Date of Birth, Education details, Address, Phone number, Work Details and so on[1-5]. They share their personal information in these sites which can be misused in many ways. They are not aware of the problems arises when this information leaked or hacked by fraudulent users. People shares the photographs in the Social media applications, and it became very common. [6][7]If one photo is uploaded, it can't be removed and stored enduringly in the database. Some fraudulent users make use of these Social sites and involved in Criminal activities. They post the photographs of other persons without their knowledge. They are collecting the unknown persons photographs in many ways such as taking photos using their mobile phones cameras without their knowledge, collecting images from Social networks, stealing images from the theft mobiles and so on. [8][9][10][11]

These users create a fake account in the Social sites, and they may set these photographs as their profile pictures to make other users trust them. Using these fake accounts, they used to give friend request to other users and joins in the group accounts. They started involving in Criminal activities without the knowledge of other users. These fraudulent users post other photographs, used for other criminal activities and the Social sites such as Facebook does not provide any security feature or having any restrictions to handle these types of situation, instead promoting the users to upload the photographs in their sites.[12][13][14]

Privacy protection is the important aspect in the Social sites. But in the above cases, the user is not aware that their photo is uploaded without their permission. There are two different scenarios in posting the photographs. The user photo will be uploaded by their friends. At the same time, the photographs should not ne uploaded by anonymous person in the Social sites. The complication of posting the photographs will become worse when other people tagged the situation. People connected in the Social sites doesn't know whether the photo is posted with the user permission or not. They simply tag and the photograph will spread by other users without knowing the risk involved in it. [15-20]

The User in the photograph totally unaware of the situation and the consequences that arises. Whenever a photograph is posted in the Social sites, user security and privacy are involved in it. Though the Users restrict themselves in posting the photographs when thinking about the privacy and security, fraudulent users posting the other user photos due to the low security mechanisms in the Social sites. So, we need a system that provides highest level of security in posting the photographs so that they should use the application and access the sites without any uncertainty about the security level especially in the posting of photographs. [21-24]

II. PROBLEM DEFINITION

Privacy and Security are the most important aspects in the Social networks. But in the Social sites such as Facebook, user's privacy and security are not maintained especially in posting the photographs. Instead of providing the security to the users, they are allowing the user to post another photograph. To attract the user and get more people involved in the application, it provides many features like Tagging.

Revised Manuscript Received on December 11, 2019.

Mary Linda, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India.

C. Anuradha Department of CSE, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India.

S. Pothumani, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India

Many fraudulent users use fake accounts in the Social sites and involving in criminal activities. They used to post other user photos without their knowledge. The Security of the user is not handled in the above situation. Without giving security measures in posting the photographs, the additional features such as Tagging make the posted photos shared all over the internet and these photographs are misused. This leads to the privacy and security violation in the Social sites.[25][26]

III. SYSTEM ANALYSIS

A. Existing system

To avoid the security problem, authors recommended Social sites application such as Facebook to use the multi-party privacy model to increase the user's security. The User should create a group where the access being granted for posting the photographs. There are some policies which are used to exemplify the users for posting of images. Privacy policy is the one in which set of users can have access of the posted photographs explicitly whereas Exposure policy involves the set of people where the photograph can be obtained when any individual person is engaged. For this, Recognition of the face in the posted photo is implemented. So, training have been given for the facial recognition system to detect the faces in the photo uploaded by the fraudulent users. In Facial recognition system, users mobile phone gallery acts as a database and are used as a training data. These data are the actual private data set of every user and the System uses them to detect and identify the faces and construct a feature vector. As the large data set is required by the system for the training purpose, it involves large computational cost. The training sets are provided manually in which the application sometimes may fail to calculate the data sets. In this method, each user will have separate training set to identify the faces in the photographs.[27-29]
The Facial recognition system have been constructed as a multi-classifier system. Several classes are used in the system in which each class belongs to individual user. The system has been built using by Binary Classifier merging where all the classes are differentiated according to the value set. For this training purposes, many samples of photographs are needed for every user, but it is not possible at every stage. [29-30]

DISADVANTAGES

1. The computational expenses are high.
2. Lots of Manual work.
3. Sharing of Photo is not secure.

B.PROPOSED SYTSEM

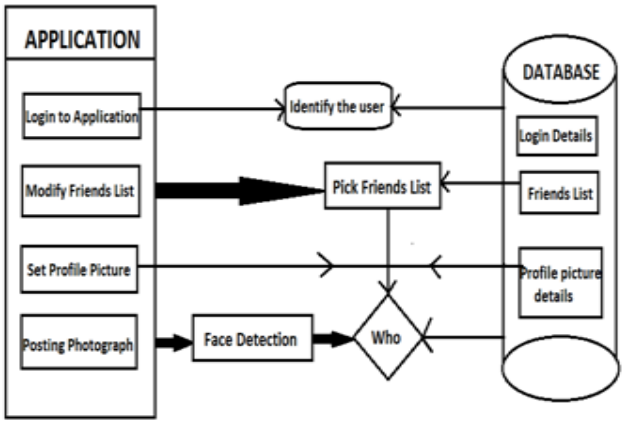
We proposed a system that provides the highest level of security in the Social sites for posting the photographs. The Social site users can have their own set of photos stored in their personal system. The User should feel highest assurance level of security and privacy when using these Social sites. The System is developed with a secure approach to ensure both efficiency and privacy of the user.

ADVANTAGES

1. Security is enhanced with less possibility of loss of information.
2. Privacy leakage of the owner's photo is prevented.
3. Sharing of Photo is trustworthy and Proficient.

IV. SYSTEM IMPLEMENTATION

The developed system contains a set of registered users and all the user's login and password credential details will be saved in the system. All the User's photographs will be saved in a common folder which acts as a Facebook database. Every user's friends list will be saved in the Facebook database. The user can able to add a friend or remove a friend and the friends list will be automatically updated. All the images are saved with the appropriate user name with the help of user login information.[31-35]



B.System Architecture

The user needs to login into the application with this username and password credentials. The user can able to upload the photograph in the application. When the user tries to post a photo in the application, the system will first recognize the person in the photograph. The System then check whether the identified person in the photograph matches with the faces in in the Facebook database. If the User uploads their own photograph, the system will detect and come to a decision that actual User's face and the detected person's face is same, and the system will allow the user to upload the photo in the application. [36-38]
If the user tries to upload other person photographs, then the system will check whether the identified person in the photograph is present in the Facebook database or not. If the identified person is not present in Facebook database, then the user is not permitted to upload the photograph in the Facebook application.
If the identified person is present in the Facebook database, the system will check whether the identified person is in user's friends list. If present, user is permitted to upload the photo. If the identified person is not present, then notification will be sent to the identified person. Thus, photographs will be posted by the right person who have access for uploading in the Social sites.

V. MODULES

A. Login Form

The User needs to register with their information in the application. After registration, the user will login with the username and password[41]. If the credentials are matched, then the user will be logged into the application. If the credentials are not matched, then the user will be displayed with the message 'Invalid Login'.

B. Setting Profile picture

The system allows the user to set their own profile picture. The User can be able to view the profile picture and they can select a new photograph from their mobile gallery. The uploaded profile picture will be saved in the system's database under the username folder, which will be used by the system to identify the faces later on.

C. Adding and Deleting Person from Friends list

Every user has their own customized friends list. Once the user selects the 'View my friends' option, the system will fetch the friends list from the database and display the user's friend list. The user can able to add new friends in the friends list by selecting 'Add a friend' option t. The system also enables the user to delete the person's name from their friends list.[38]

E. Posting the photograph

The User can post the photograph in the application. Once the user uploads the photo, the System will identify the faces in the photo. The System will check the application database to find the matching photograph. If the User uploads their own photo, the system will find the face in the database and displays the detected person's face with a message 'Your photo is uploaded'. Thus, the system will allow the user to upload their own photo in the application.

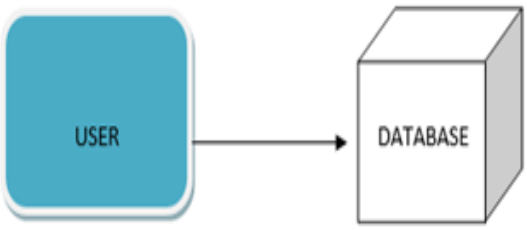
If the user tries to upload other person photographs, then the system will check whether the identified person in the photograph is present in the application database or not. If the identified person is not present in application database, then the user is not permitted to upload the photograph in the Facebook application by displaying the message 'User is not in application database'.[39]

F. Notification

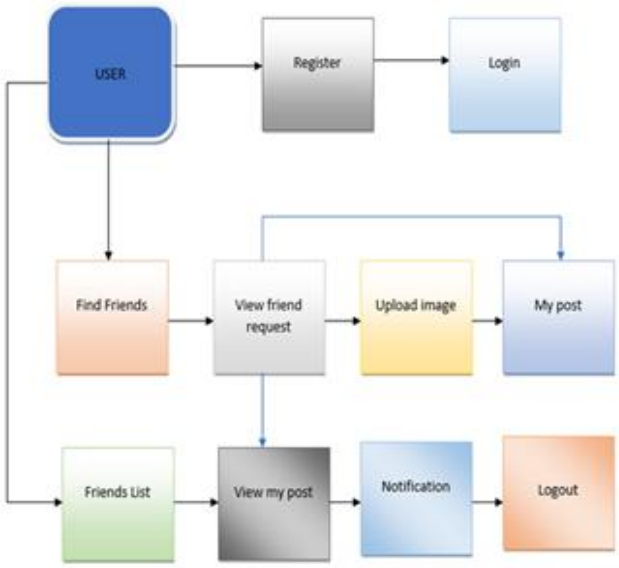
If the user tries to upload other person photographs, then the system will check whether the identified person in the photograph is present in the application database or not. If the identified person is present in the Facebook database, the system will check whether the identified person is in user's friends list. If present, user is permitted to upload the photo. If the identified person is not present, then notification will be sent to the identified person. Thus, photographs will be posted by the right person who have access for uploading in the Social sites.[40]

VI. DATA FLOW DIAGRAM

LEVEL 0:

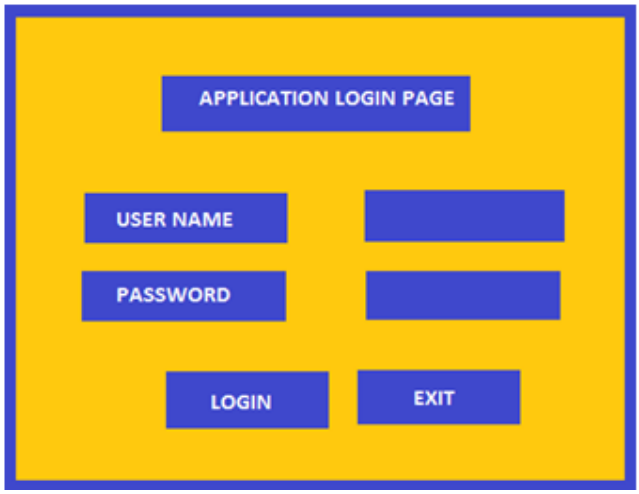


LEVEL 1:

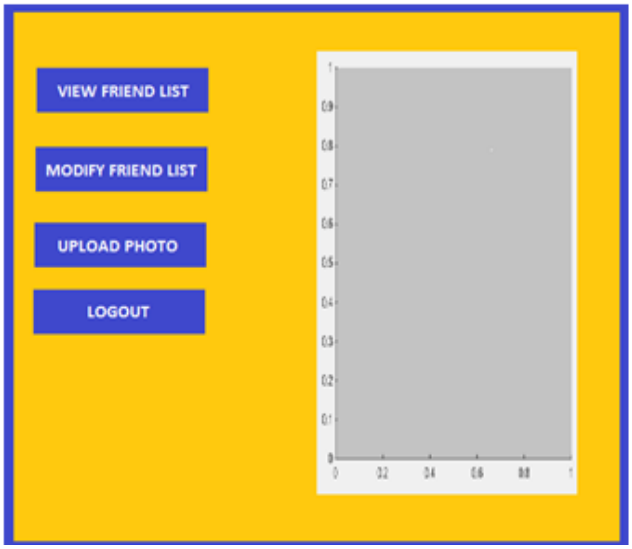


VII. RESULTS

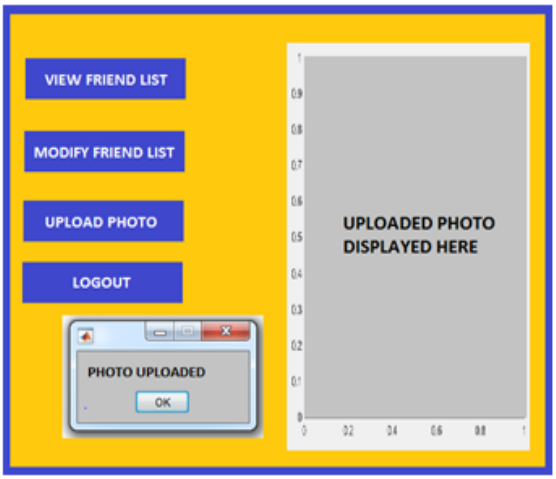
A. Application Login Page



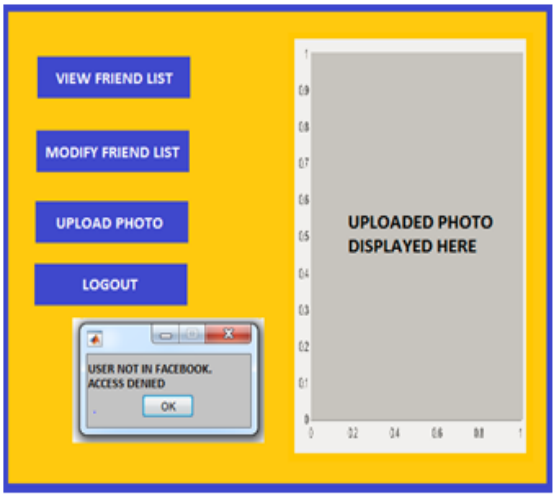
B. User Home Page



C. User Uploading own photograph

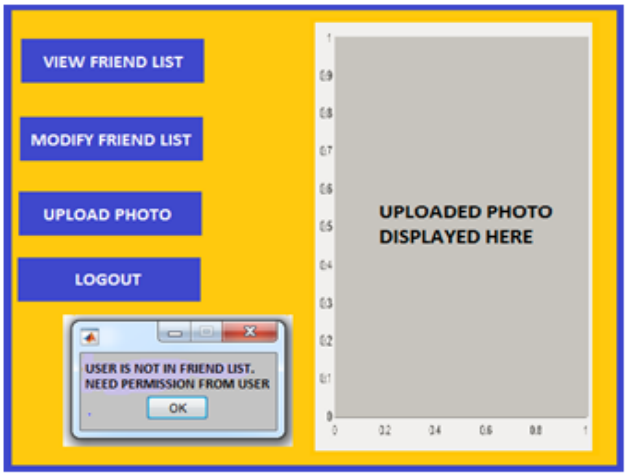


D. User Uploading Other Person's Photo not in Facebook

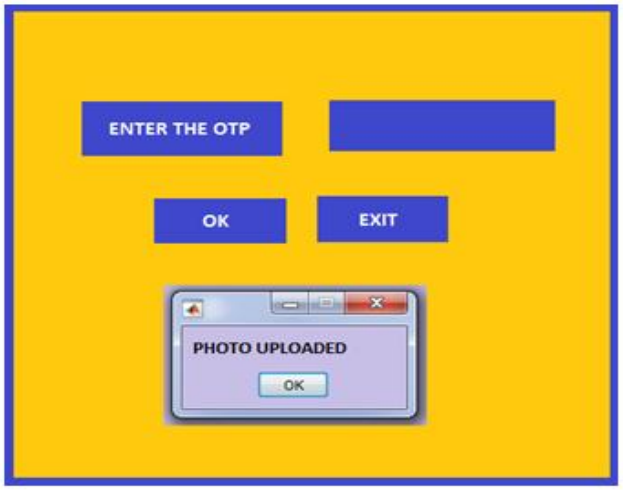


E. User Uploading Friend's Photo

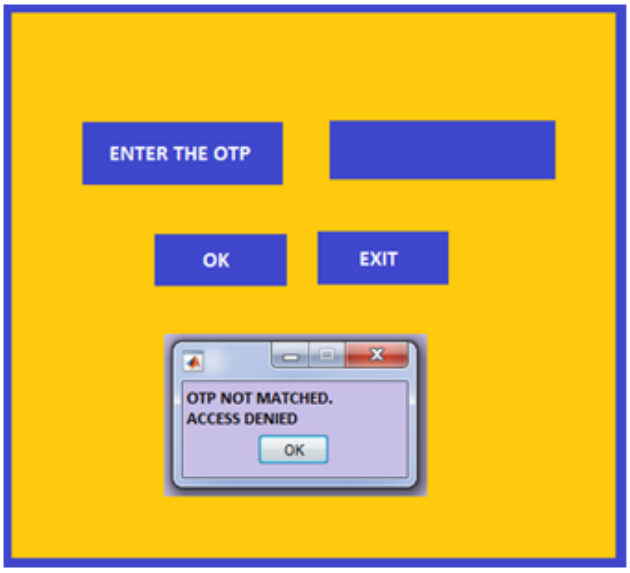
F. User Uploading Other Person's Photo not in Friend list



G. Notification Page – Enters Correct OTP



H. Notification Page – Enters Incorrect OTP



VIII. CONCLUSION

Uploading the photographs is one of the most common activity in the Social media applications such as Facebook. But the privacy is leaked if the photo is uploaded without the user knowledge. To avoid this security problem, we developed an efficient face recognition system to identify the user in the photograph. If the identified person is not in the Facebook, the user is not allowed to post the photo. If the identified person is not present in the user friend list, then the user should get permission from the identified person to upload the photo. We expect that the developed system useful in user's secrecy and privacy of photographs in the Social media applications. Proposed future work could be how the photo samples will be moved to clouds like Dropbox.

REFRENCES

[1] Kumarave A., Rangarajan K.,Algorithm for automaton specification for exploring dynamic labyrinths,Indian Journal of Science and Technology,V-6,I-SUPPL5,PP-4554-4559,Y-2013
[2] P. Kavitha, S. Prabakaran "A Novel Hybrid Segmentation Method with Particle Swarm Optimization and Fuzzy C-Mean Based On Partitioning the Image for Detecting Lung Cancer" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June 2019
[3] Kumaravel A., Meetei O.N.,An application of non-uniform cellular automata for efficient cryptography,2013 IEEE Conference on Information and Communication Technologies, ICT 2013,V-,I-,PP-1200-1205,Y-2013
[4] Kumarave A., Rangarajan K.,Routing alogrithm over semi-regular tessellations,2013 IEEE Conference on Information and Communication Technologies, ICT 2013,V-,I-,PP-1180-1184,Y-2013
[5] P. Kavitha, S. Prabakaran "Designing a Feature Vector for Statistical Texture Analysis of Brain Tumor" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June 2019
[6] Dutta P., Kumaravel A.,A novel approach to trust based identification of leaders in social networks,Indian Journal of Science and Technology,V-9,I-10,PP--,Y-2016
[7] Kumaravel A., Dutta P.,Application of Pca for context selection for collaborative filtering,Middle - East Journal of Scientific Research,V-20,I-1,PP-88-93,Y-2014
[8] Kumaravel A., Rangarajan K.,Constructing an automaton for exploring dynamic labyrinths,2012 International Conference on Radar, Communication and Computing, ICRCC 2012,V-,I-,PP-161-165,Y-2012
[9] P. Kavitha, S. Prabakaran "Adaptive Bilateral Filter for Multi-Resolution in Brain Tumor Recognition" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8 June, 2019
[10] Kumaravel A.,Comparison of two multi-classification approaches for detecting network attacks,World Applied Sciences Journal,V-27,I-11,PP-1461-1465,Y-2013
[11] Tariq J., Kumaravel A.,Construction of cellular automata over hexagonal and triangular tessellations for path planning of multi-robots,2016 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2016,V-,I-,PP--,Y-2017
[12] Sudha M., Kumaravel A.,Analysis and measurement of wave guides using poisson method,Indonesian Journal of Electrical Engineering and Computer Science,V-8,I-2,PP-546-548,Y-2017
[13] Ayyappan G., Nalini C., Kumaravel A.,Various approaches of knowledge transfer in academic social network,International Journal of Engineering and Technology,V-,I-,PP-2791-2794,Y-2017
[14] Kaliyamurthie, K.P., Sivaraman, K., Ramesh, S. Imposing patient data privacy in wireless medical sensor networks through homomorphic cryptosystems 2016, Journal of Chemical and Pharmaceutical Sciences 9 2.
[15] Kaliyamurthie, K.P., Balasubramanian, P.C. An approach to multi secure to historical malformed documents using integer ripple transfiguration 2016 Journal of Chemical and Pharmaceutical Sciences 9 2.
[16] A.Sangeetha,C.Nalini,"Semantic Ranking based on keywords extractions in the web", International Journal of Engineering & Technology, 7 (2.6) (2018) 290-292
[17] S.V.GayathiriDevi,C.Nalini,N.Kumar,"An efficient software verification using multi-layered software verification tool "International Journal of Engineering & Technology, 7(2.21)2018 454-457
[18] C.Nalini,ShwtambariKharabe,"A Comparative Study On Different Techniques Used For Finger – Vein Authentication", International Journal Of Pure And Applied Mathematics, Volume 116 No. 8 2017, 327-333, Issn: 1314-3395
[19] M.S. Vivekanandan and Dr. C. Rajabhushanam, "Enabling Privacy Protection and Content Assurance in Geo-Social Networks", International Journal of Innovative Research in Management, Engineering and Technology, Vol 3, Issue 4, pp. 49-55, April 2018.
[20] Dr. C. Rajabhushanam, V. Karthik, and G. Vivek, "Elasticity in Cloud Computing", International Journal of Innovative Research in Management, Engineering and Technology, Vol 3, Issue 4, pp. 104-111, April 2018.
[21] K. Rangaswamy and Dr. C. Rajabhushanamc, "CCN-Based Congestion Control Mechanism In Dynamic Networks", International Journal of Innovative Research in Management, Engineering and Technology, Vol 3, Issue 4, pp. 117-119, April 2018.
[22] Kavitha, R., Nedunchelian, R., "Domain-specific Search engine optimization using healthcare ontology and a neural network backpropagation approach", 2017, Research Journal of Biotechnology, Special Issue 2:157-166
[23] Kavitha, G., Kavitha, R., "An analysis to improve throughput of high-power hubs in mobile ad hoc network" , 2016, Journal of Chemical and Pharmaceutical Sciences, Vol-9, Issue-2: 361-363
[24] Kavitha, G., Kavitha, R., "Dipping interference to supplement throughput in MANET" , 2016, Journal of Chemical and Pharmaceutical Sciences, Vol-9, Issue-2: 357-360
[25] Michael, G., Chandrasekar, A.,"Leader election based malicious detection and response system in MANET using mechanism design approach", Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016 .
[26] Michael, G., Chandrasekar, A.,"Modeling of detection of camouflaging worm using epidemic dynamic model and power spectral density", Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016 .
[27] Pothumani, S., Sriram, M., Sridhar, J., Arul Selvan, G., Secure mobile agents communication on intranet,Journal of Chemical and Pharmaceutical Sciences, volume 9, Issue 3, Pg No S32-S35, 2016
[28] Pothumani, S., Sriram, M., Sridhar , Various schemes for database encryption-a survey, Journal of Chemical and Pharmaceutical Sciences, volume 9, Issue 3, Pg NoS103-S106, 2016
[29] Pothumani, S., Sriram, M., Sridhar, A novel economic framework for cloud and grid computing, Journal of Chemical and Pharmaceutical Sciences, volume 9, Issue 3, Pg No S29-S31, 2016
[30] Priya, N., Sridhar, J., Sriram, M. "Ecommerce Transaction Security Challenges and Prevention Methods- New Approach" 2016 ,Journal of Chemical and Pharmaceutical Sciences, JCPS Volume 9 Issue 3.page no:S66-S68 .
[31] Priya, N.,Sridhar,J.,Sriram, M."Vehicular cloud computing security issues and solutions" Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016
[32]Priya, N., Sridhar, J., Sriram, M. "Mobile large data storage security in cloud computing environment-a new approach" JCPS Volume 9 Issue 2. April - June 2016
[33] Anuradha.C, Khanna.V, "Improving network performance and security in WSN using decentralized hypothesis testing "Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016 .
[34]Anuradha.C, Khanna.V, "A novel gsm based control for e-devices" Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016 .
[35]Anuradha.C, Khanna.V, "Secured privacy preserving sharing and data integration in mobile web environments " Journal of Chemical and Pharmaceutical Sciences(JCPS) Volume 9 Issue 2, April - June 2016 .
[36]Sundarraj, B., Kaliyamurthie, K.P. Social network analysis for decisive the ultimate classification from the ensemble to boost accuracy rates 2016 International Journal of Pharmacy and Technology 8
[37]Sundarraj, B., Kaliyamurthie, K.P. A content-based spam filtering approach victimisation artificial neural networks 2016 International Journal of Pharmacy and Technology 8 3.

[38]Sundarraj, B., Kaliyamurthie, K.P. Remote sensing imaging for satellite image segmentation 2016 International Journal of Pharmacy and Technology 8 3.
[39]Sivaraman, K., Senthil, M. Intuitive driver proxy control using artificial intelligence 2016 International Journal of Pharmacy and Technology 8 4.
[40]Sivaraman, K., Kaliyamurthie, K.P. Cloud computing in mobile technology 2016 Journal of Chemical and Pharmaceutical Sciences 9 2.
[41]Sivaraman, K., Khanna, V. Implementation of an extension for browser to detect vulnerable elements on web pages and avoid click jacking 2016 Journal of Chemical and Pharmaceutical Sciences 9 2.

AUTHORS PROFILE

I. Mary Linda, Assistant Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India

C. Anuradha Assistant Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India

S. Pothumani, Assistant Professor, Department of Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, India