ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Identification of Anonymous Identical Users in Multiple Social Media Networks

R.Thenmozhi[1], P.Ananthi[2], R.Divya[3], C.Lavanya[4], K.Livya[5]

Asst. Prof, Dept. of Information Technology, Valliammai Engineering College, Chennai, India[1]

U.G Students, Dept. of Information Technology, Valliammai Engineering College, Chennai, India[2,3,4,5]

ABSTRACT: Many types of social networking sites have emerged and contributed immensely to large volumes of real-world data. Online Social Networks(OSN) allow users to create a public or private profile, encourage people to share information and interests with other people and communicating with each other. As a result, OSNs are being used by millions of people and they are now part of our everyday life. People use OSNs to keep in touch with family, friends, and share personal information, as well as for business purposes. Users of an OSN build connections with their friends, relatives, colleagues and people over time. Although a dramatic increase in OSN usage like Facebook, there is a lot of security and privacy concerns. Attackers harass their victims by posting sexual remarks, threats, or repeated hurtful messages[1]. Also, attackers spread cruel rumours about the victims and share embarrassing pictures or videos of the victims in the network. In addition, the majority of this kind of attack happened in OSN sites. Cyberbullying attack is one of the abuse behavior in the Internet as well as a very serious social problem[3]**.**The proposed system compares the behavioural patterns of users with the data sets in the database to find the anomalous behaviours and also predict the unwanted message shared by the person through the Social media networks and block their ID. To integrate users of various community a probabilistic-clustering approach is used. Support Vector Machine (SVM) Classification algorithm is used to predict the unwanted message/pictures shared by the person through the Social media networks.

KEYWORDS*:* Online Social Networks(OSN), Support Vector Machine(SVM),Anomalous behaviour.

I.INTRODUCTION

Online Social Networks (OSNs) has become the major media that allow users to create a public or private profile, encourage sharing information and their opinion from virtual community, forums, Blog to Social Network Services (SNS). Social media helps people to communicate with each other without any boundary. People use OSNs to keep in touch with family, friends, and share personal information, as well as for business purposes. Users of an OSN build connections with their friends, colleagues and people over time. These connections form a social graph that controls how the information spreads in various social media network. More precisely, an online social networks (OSNs) is an online platform that provides social networking services for a user. Despite the popularity of centralized OSNs, the users privacy and control over their data is becoming a major issue for these social networking services. In general, attackers use the OSN infrastructure to collect and expose personal information about a user and their friends. Cyberbullying has become quite common in online social networks. Attackers harass their victims (usually children and teenagers) by posting sexual remarks, threats, or repeated hurtful messages. Also, attackers spread cruel rumors about the victims and share embarrassing pictures or videos of the victims in the network[1]. A recent study discovered that 12% of parents claim their child has been cyberbullied. In addition, the majority of this kind of attack happened in OSN sites like Facebook. To prevent people from this attack, the proposed system uses Support Vector Machine algorithm[12] that predicts the unwanted message shared by the person through the social media network and block the id of the anonymous user.

DOI: 10.15680/IJIRCCE.2019. 0702034

II. OBJECTIVES

1. Find anonymous users and attackers harassing their victims.
2. Predict the unwanted message shared by the person through the Social media networks.
3. Block the anonymous user ID by comparing the content posted by users with stored data set.

III. RELATED WORK

3.1CONNECTING USERS ACROSS SOCIAL MEDIA SITES: A BEHAVIOURAL MODELLING APPROACH:

Many people use various social media where, the information on an individual site is often incomplete. When sources of complementary information are integrated, a improved profile of a user can be built to expand online authenticating online information facilities. It is needed to find individuals across social media places. A methodology Modelling Behaviour for Identifying Users across Site (MOBIUS) for discover a mapping among identities of personalities[2]. It comprises of three key works: the first module identifies users' unique behavioural designs that lead to provide information redundancies across sites; the second module constructs the features that exploit information redundancies due to these interactive patterns; and the third component employs device learning for effective user documentation. We define the cross-media user identification problem and show that MOBIUS is operative in identifying users across social media sites. This learning provides the way for examine and mining across social media sites.

3.2TOWARDS THE DETECTION OF CYBERBULLYING BASED ON SOCIAL NETWORK MINING TECHNIQUES:

Cyberbullying is one of the most frequently happen Internet abuse and also a very serious social problem especially for teenager**.** In this paper, we studied an approach based on social networks analysis and data mining for cyberbullying detection. There are three main techniques for cyberbullying discovery, including keyword matching technique, opinion mining and social network analysis[3].The simplest one is based on dictionary which collect a set of keywords that related to cyberbullying. Some advanced techniques including intelligent tag based approach, machine learning and artificial intelligence approach, such as genetic algorithm or neural network. First is the behaviour model of cyberbullyer and second is tone and sentiment of the speak on Internet. Social Networks Mining (SNM) is a new research area which is developed by combing Social Network Analysis and Data Mining.

3.3FAKEBOOK: DETECTING FAKE PROFILES IN ON-LINE SOCIAL NETWORKS:

On-line Social Networks (OSNs) help people to communicate with each other and share their personal, professional and political information which increases the reports on security and privacy threats in the OSNs.SMN having tens or hundreds of million users collectively generating billions of personal data content that can be exploited, detecting and preventing attacks on individual user privacy is a major challenge. The risk is due to the fact that an adversary may create a fake profile to impersonate a real person that leads to various attacks like Identity Cloning Attack(ICA) and fake profile attack(FPA)[4].The fake profile could be exploited to build online relationship with the friends of victim of identifying theft, with the final target of stealing personal information of the victim, via interacting with the friends of the victim. In this paper, the investigation to mitigate this problem by analyzing the social network graphs from a dynamic point of view based on dataset, evolution over time of the number of friends and Real life social network based verification.

3.4 CROSS-SYSTEM USER MODELING AND PERSONALIZATION ON THE SOCIAL WEB:

The Social media provides opportunities to gather various types of user data. Aggregated user data depends on the nature of individual user profiles distributed on the Social Web. In this paper, we study distributed form-based and tag-based user profiles, based on a large dataset aggregated from the Social Web. We analyze the consistency of form-based profiles, that the users explicitly create by filling out forms at Social Media such as Twitter, Facebook and LinkedIn. We also investigate tag-based profiles[5], which result from social tagging activities in systems such as Flickr, Delicious and StumbleUpon: to what extent do tag-based profiles overlap between different systems based on the insights that are developed and evaluated the performance of several cross-system user modelling strategies.

3.5 USER PROFILE MATCHING IN SOCIAL NETWORKS:

The web is not only used to read information, but also it is used as a social tool for users.Inter-social networks operations and functionalities are used in several scenarios. To achieve this, matching user profiles is required. Matching user profiles on social networks suffers from three main problems based on Social Network Representations, User Profile Domains and Site/User Objectives[6].Current methods of matching user profile is restrictive and do not consider all the related problems. Particularly, it assumes two profiles describe the same physical person only if the values of their Inverse Functional Property or IFP (e.g. the email address, date-of-birth, etc.) are the same. we address the problem of matching user profiles in its globality by providing a suitable matching framework for all the profile attributes.

IV. PROPOSED ALGORITHM

SUPPORT VECTOR MACHINE ALGORITHM

It is classification algorithm is used to predict and block the unwanted content shared by person through the social media network. When the user post a status it goes under following steps

MAPPING AND ASSEMBLY:

In mapping and assembly a standard model is specified for each object, which is defined by the framework. Mapping technique maps the posted content with the database and then assemble process occurs by splitting the content.

PRE-FILTERING:

The assembled post is pre-filtered by using two methods stopwords and stemming techniques. Stopwords are used to remove the words like is, was, at, for whereas the stemming techniques is used to reduce inflected words to their root form.

COMPARISION:

The filtered status is comparing with a blacklist in the database.Then keywords are allowed to check with the database then it says the content is bad or good.

V. ARCHITECTURE DIAGRAM

When the new user wants to enrol into this system, they have to register theirnew credentials like name,email id, username , password and mobile number**.** Then theusers can login into the system by entering the accurate username and password .All these credentials and the unwanted messages and photos are stored in database. Now, the user post their status(message or photos) in their timeline. The system matching the patterns of posted content and the content stored in database if, the posted content is matched with the content in database based on the Support Vector Machine Based Spam Detection it blocks the user ID else the posted content is shared into the timeline of the user.

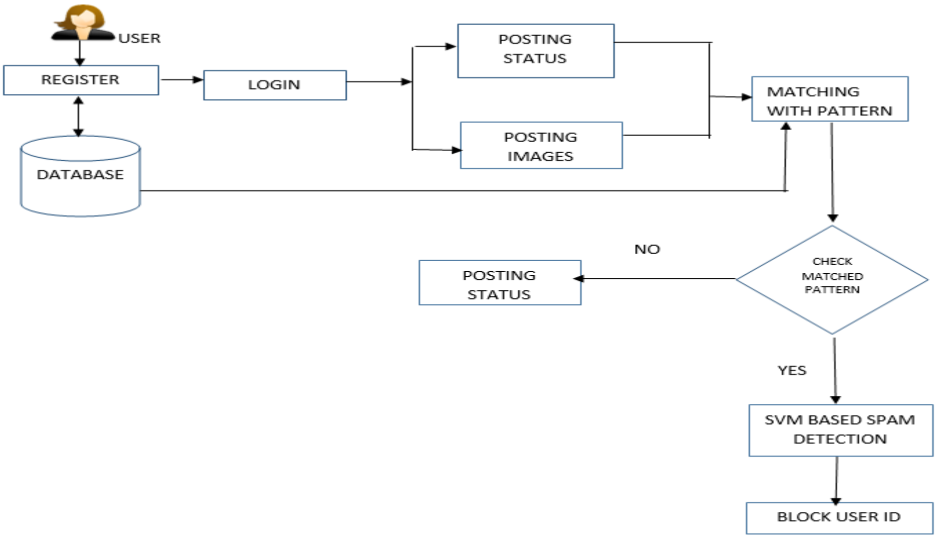

Fig -1: Overall Architecture Diagram

VI. MODULAR DESCRIPTION

A.USER REGISTRATION:

Users can login into the system if the user is already existing otherwise the user enter the accurate username and password. The user can Register with the new credentials like name ,email id, username , password ,mobile no and then go the login page enter the particulars then advance the process.

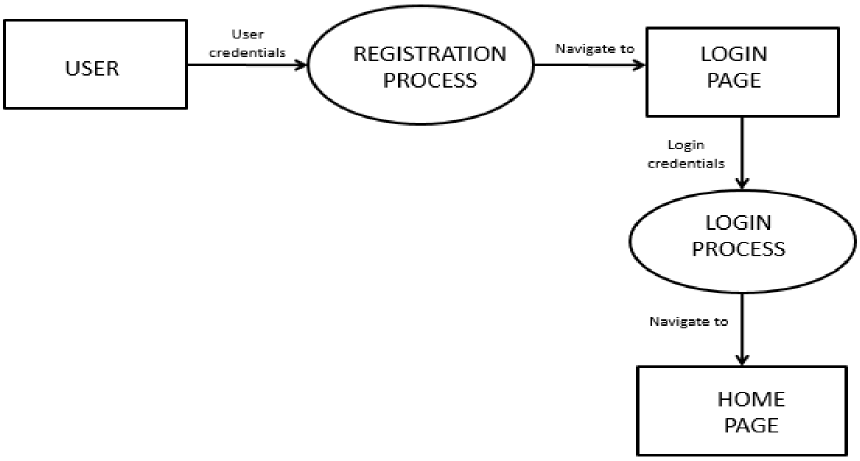

Fig -2: Flow Diagram for User Registration

B.FRIEND REQUEST PROCESS:

Friend request process enable user to send friend request to the known user. Find the individual details by using exploration bar. Individual identify the particulars of the friend then he/she will agree or discard the friend request .if the friend accept the request then that person is added to friends circle.

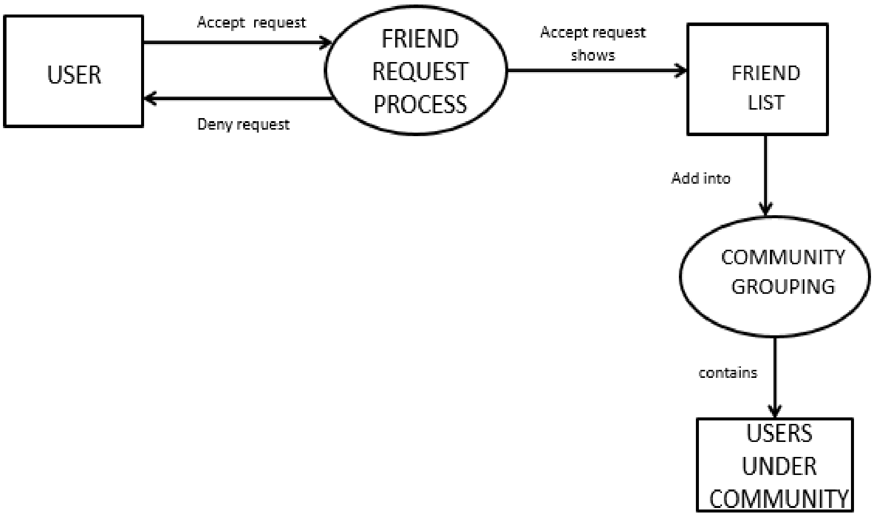

Fig -3: Flow Diagram for friend request process

DOI: 10.15680/IJIRCCE.2019. 0702034

C.ANNOYING POST IDENTIFICATION:

The message from your friend is identified as either welcome or unwelcome. If the message is unwelcome means the system will reject the message automatically.It means all the friends see the beneficial messages only.It also identifies the person who post repetitively unwanted message to the system.

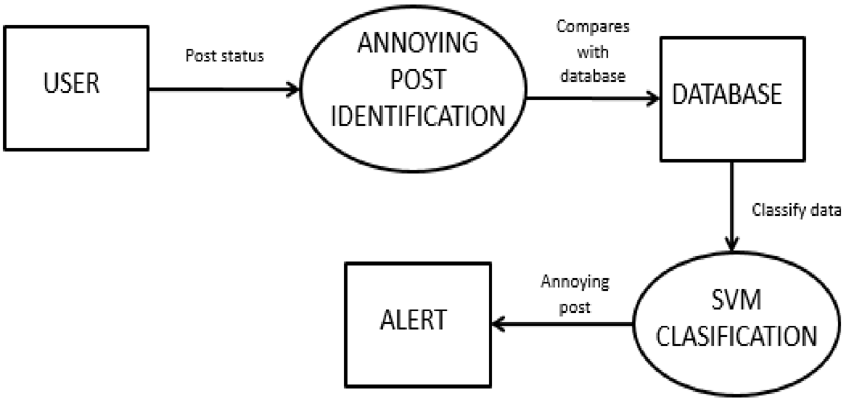

Fig -4: Flow Diagram for Annoying post Identification.

D.**BLOCK THE USER ID**:
Data is classified based on SVM classifier knowledge and based on the decision value messages will be classified.The pattern of messages or images is recognized and matched with the data which is in the database.Then the anonymous messages or images will be blocked automatically before the user views it.

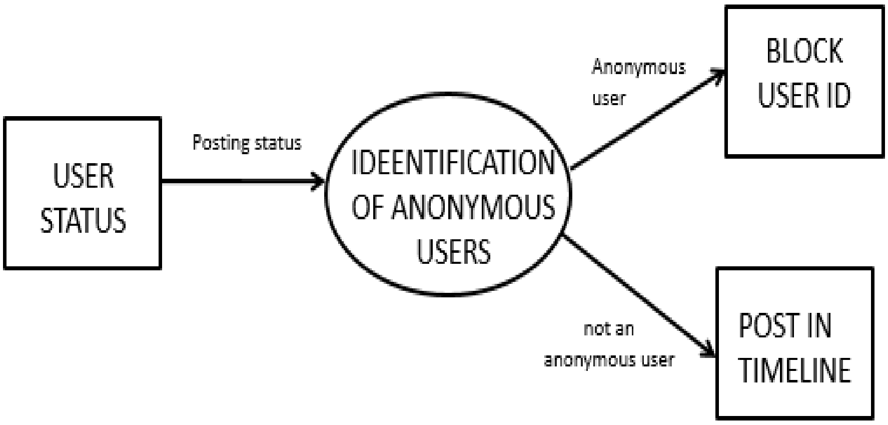

Fig -5: Flow Diagram for block user ID.

VII. FUTURE WORK

The day by day increase in usage of Online social media network will also be used for both good and purpose. To prevent the users from the annoying others this system accounts on Identification of anonymous user on the social media network with the proposed system. By including this feature it helps the users to block the anonymous users immediately and automatically. Thus, the anonymous activity on the social media network will be reduced to a greatest extent. we havesome future directions to proceed the research and to study the situation by applying this approach to different countries and culture. We believe that some interesting results will be discovered, which will be helpful for us to improve the performance in identifying the anonymous users.

VIII. CONCLUSION

Identifying anonymous users across multiple Social Media Network is difficult task. This investigation designed the motivation for more examinations on the issues of existing system. The diverse users with totally different characteristics can be analysed before posting the annoying post to the other users. Thus, it prevent the unanonymous users include children, teenagers and adults from the attack of cyberbulling. Our solution can be easily identified and applied to any social media networks including Twitter, facebook, Instagram etc.., It can also be extended to other studies in the field of social computing with cross-application problems. other user identification methods can be applied simultaneously to study various social media application.

REFERENCES

[1] Naeimeh Laleh, Barbara Carminati and Elena Ferrari, “Risk Assessment in Social Networks based on User Anomalous Behaviours,” DOI 10.1109/TDSC.2016.2540637, IEEE Transactions,2018.

[2] R. Zafarani and H. Liu, "Connecting users across social media sites: a behavioral-modeling approach, " Proc. of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD’13), pp.41-49, 2013.

[3] I-Hsien Ting,Wun Sheng Liou,Dario Liberona,Shyue-Liang Wang,Giovanny MauricioTarazona Bermudez, ”Towards the Detection of Cyberbullying Based on Social Network Mining Techniques,” IEEE International Conference on Behavioral, Economic, Socio-cultural Computing (BESC),2018.

[4] Mauro Conti, Radha Poovendran, Marco Secchiero, “FakeBook: Detecting Fake Profiles in On-line Social Networks,” IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining,2012.

[5] F. Abel, E. Herder, G.J. Houben, N. Henze, and D. Krause, "Cross-system user modeling and personalization on the social web," User Modeling and User-Adapted Interaction, vol. 23, pp. 169-209, 2013.

[6] E. Raad, R. Chbeir, and A. Dipanda, "User profile matching in social networks," Proc. Of the 13th International Conference on Network-Based Information Systems (NBiS’10), pp.297-304, 2010.

[7] A. Acquisti, R. Gross and F. Stutzman, "Privacy in the age of augmented reality," Proc. National Academy of Sciences, 2011.

[8] T. Iofciu, P. Fankhauser, F. Abel, and K. Bischoff, "Identifying users across social tagging systems,” Proc. of the 5th International AAAI Conference on Weblogs and Social Media, pp. 522-525, 2011.

[9] M. Motoyama and G. Varghese, "I seek you: searching and matching individuals in social networks," Proc. of the 11th international workshop on Web Information and Data Management (WIDM’09), pp. 67-75, 2009.

[10] A. Narayanan and V. Shmatikov, "De-anonymizing social networks," Proc. Of the 30th IEEE Symposium on Security and Privacy (SSP’09), pp. 173-187, 2009.

[11] K. Cortis, S. Scerri, I. Rivera, and S. Handschuh, "An ontology based technique for online profile resolution," Social Informatics, Berlin: Springer, pp. 284-298, 2013.

[12] Kuldeep Yadav, Swetank K. Saha, Ponnurangam Kumaraguru, Rohit Kumra, “Take Control of Your SMSes : Designing an Usable Spam SMS Filtering System”,IEEE 13th International Conference on Mobile Data Management,2012.

[13] J. Vosecky, D. Hong, and V.Y. Shen, "User identification across multiple social networks," Proc. Of the 1st International Conference on Networked Digital Technologies, pp.360-365, 2009.

[14] P. Jain, P. Kumaraguru, and A. Joshi, "@ i seek 'fb. me': identifying users across multiple online social networks," Proc. of the 22nd International Conference on World Wide Web Companion, pp. 1259-1268, 2013.

[15]P. Jain and P. Kumaraguru, "Finding Nemo: searching and resolving identities of users across online social networks," arXiv preprint arXiv:1212.6147, 2012.

[16] M. Almishari and G. Tsudik, "Exploring linkability of user reviews," Computer Security–ESORICS 2012 (ESORICS’12), pp. 307- 324, 2012.

[17] X. Kong, J. Zhang, and P.S. Yu, "inferring anchor links across multiple heterogeneous social networks," Proc. of the 22nd ACM International Conf. on Information and Knowledge Management (CIKM’13), pp. 179-188, 2013.

[18] O. Goga, H. Lei, S.H.K. Parthasarathi, G. Friedland, R. Sommer, and R. Teixeira, "Exploiting innocuous activity for correlating users across sites," Proc. 22nd international conference on World WideWeb (WWW’13),pp. 447-458, 2013.