# RECOMMENDING A RELIABLE FRIEND IN ONLINE SOCIAL NETWORK USING SEMANTIC ANALYSIS

**G. Thamizhamudhu** [1]

[1]*M.Tech student, Dept of CSE, Pondicherry Engineering College, Pondicherry.*
*Email: tamilgopal3@pec.edu*

**J. Jayabharathy**[2]

[2]*Associate Professor, Dept of CSE, Pondicherry Engineering College, Pondicherry.*
*Email: bharathyraja@pec.edu*

***Abstract:*** *Online Social Network(OSN) is a platform, where users are able to share information among them easily and instantly. The sensitive information of an user can be misused by his/her friends or friends of friends due to the lack of Friend Request Acceptance (FRA) and Reliable FRA (also known as Reliable Decision Making), which is one of the key issues in OSNs. The existing FRA techniques are functioning based on Blind (method, where user used to accept friend requests without knowing information of friend-to-be), Manual Search (method, accept friend requests by complying identical attributes with friend-to-be or confirming by the timeline, if profile is public) and Prospect to become friend (method, considers the matching factor using the same attributes of the user and friend-to-be). Reliable Decision Making (RDM) is a function that determines the reliable friend based on the following parameters, such as security, flexibility, effectiveness and satisfaction. A approach is to bring down the misused information by filtering FRA and RDM using a reliable method to find out more information about the friend-to-be. This motivated us to propose a method for reliable decision making (RDM) of accepting friend request with added technical attributes to the algorithm in the existing system and also analyze the person's social behaviour as positive, negative and neutral through semantic analysis. The objective of the proposed system is to recommend a reliable friend in Online Social Network considering the hobbies, qualification and their behaviour.*

***Keywords:*** *Reliable Decision Making, Friend Request Acceptance, Online Social Network, Semantic Analysis, Sentimental Analysis.*

## I. INTRODUCTION

An **online social network** (OSN) is a **social** communicative medium created by the individuals or Groups of people or organizations. It (OSN) is a medium where people are allowed to share personnel, their interests and activities. It is used to facilitate **social** interaction with others of a common interest.

OSN allows registered users to create profiles, send messages, update status, upload photos and videos to connect with family members, friends and business associates. It works on the basis of Nodes and Links. The

nodes are the contents of the individuals/organisation. The link is the exchange of information through technology.

In spite of more and more advantages of OSN, it is unsafe to share sensitive information in online, i.e., time-related information, personal characteristics and activities, and user's habits. Such sensitive information is targeted by illegal users, who are involved in malpractice for unwanted purposes such as robbery, kidnapping, stalking, etc.

Now-a-days, the ever growing internet technologies led to enormous growth of the OSNs. Some of the today's OSNs are Facebook, Twitter, LinkedIn, WhatsApp, Instagram, Google+, etc.

The Facebook is the largest online social network, which can be accessed from devices with internet connectivity. The proper registration has to be done by the user in the Facebook. After registering, users can create a profile, post texts, photos, videos and etc. Also, share it with other users as "friends". It has over 2.30 billion (approx.) active users.

In Facebook, OSNs users give an access to their personal information to other people, from old friends to strangers. It may leads to cause the user in danger. As a consequence, the sensitive information of the user can be misused by friends or friends of friends due to the lack of reliable Friend Request Acceptance (FRA), which is one of the key issues in OSNs.

The existing FRA techniques are as follows:

1) Blindly Acceptance,
2) Manual Search Acceptance
3) FRA by Reliable Decision Making.

**1. Blind Acceptance**

In this method, the user used to accept friend requests blindly that is, without having to know any information about friend-to-be. The attributes of friend-to-be are being used in this method are i) Name ii) Profile Picture and Name iii) Profile Picture, Name and Mutual Friend. In Common, two attributes are being displayed on friend requests of a friend-to-be.

This method is easy and very quick. It only needs to place the confirmation after receiving the friend request. It is extremely unsafe to make friend with strangers without knowing their credentials.

**2. Manually Search Acceptance**

In this method, the user used to accept friend requests by complying identical attributes with friend-to-be. Further, the information of friend-to-be is acquired by confirming the timeline.

In some cases, the acquisition of information can be restricted if the friend-to-be set their profile is being private. This method is complex and time consuming.

**3. FRA by Reliable Decision Making.**

The Reliable Decision Making (RDM) means that if a user takes a decision for accepting friend-to-be based on the matching factor. In this method, an automated filtering algorithm is used to restrict the friends by estimated matching factor. This is reasonable as a person's behaviour, attitude and the related attributes are directly influenced by the

friends. This method is more reliable than the Blindly Acceptance and Manual Search Acceptance. However, this is not a complete method to avoid negative minded, fake or illegal friends.

**Proposed Method**

To overcome the above said issue, this paper find out another method to fulfil all the reliable sources to accept a friend request of friend-to-be by Semantic Analysis approach. **Semantic Analysis** deals with the understanding of data under various logical meanings rather than preset categories of positive or negative or neutral. It comprises of extracting relevant meanings from the given piece of information about friend-to-be.

This paper is organized as follows:

Section II - Related works.

Section III - The features of Friend Requests, along with the existing methods of friend request acceptance.

Section IV - The proposed reliable method.

Section V - The Research method

Section VI - The Experimental Result

Section VII – Conclusion.

## II. RELATED WORK

There are several related works had been done on OSNs with security, trust, discovering friendship and conserving privacy. In security point of views, there are works [1]–[5] that consider adversaries' attack on OSNs users' identities, attributes, as well as their social relationships. Adversaries can belong to existing social relationship or be strangers/fraudulent users [6]. Fong et al. [7] proposed an access model that formalized and generalized the privacy preservation mechanism for Facebook. Carminati et al. proposed an access control mechanism for the information sharing in web-based social networks in [8]. The major difference between the proposed method and [7] is that they used the decentralized architecture for the access control, which may invite potential security breaks (e.g., forming an identity, attributes, and trust information). Object Recommendation and Link Recommendation are the two different methods for recommending a friend to accept. Social networking sites such as Facebook and Twitter focus on link recommendation where friend recommendations are presented to users. Kuan et al. proposed an algorithm to locate groups using a transitive extension based approach [9].

This research work uses of a 1.5 clique extension method to derive sub structures, or communities within social networks. Results show that this method was fairly effective in finding community of friends. Research by Leskovec, et. al., emphasized the relevance and effectiveness of multi objective functions in recommendation algorithms [10].

However, similarly to Lipczak and Milios, the focuses on community detection. An analysis on brain networks using multi objective functions was per formed by Santana, et. al [11].

The most important objective of recommended systems is to estimate the ratings for the items that are new for a user [12].

Ultimately, after calculating the estimated rates for the yet unrated items, an

ordered list of most related items can be prepared and suggested to the target user. A number of previous studies have revealed the contribution of recommended systems in education. A collaborative filtering method was used in a research to recommend documents that will either encourage the users to expand their knowledge of a given topic [13].

## III. THE FEATURES OF FRIEND REQUESTS, ALONG WITH THE EXISTING METHODS OF FRIEND REQUEST ACCEPTANCE.

The following describe the features of friend request on OSNs and the existing OSNs FRA methods, which need to be discussed for designing a new reliable FRA Method. There are several features are available in OSNs, which are explained below:

**1) Friend Request Setting**

A user can adjust the preference for accepting friend by exploiting Friend Request Setting (FRS). FRS offers two types of feature such as ‘‘Everyone’’ and ‘‘Friends of Friend’’. The first one indicates that every user on a particular OSN platform can become a user’s friend. The Second one, indicates that only the friends of a user’s friends can become the friend. It limits friend requests to the users who are not interested to make random friends. It also can assist a user to keep information private and secure compared to the former one [14].

**2) Find Friend**

A user can be connected with the old/new friends utilizing this feature. It can help to generate a list of people and their profiles according to the user’s provided information such as name, hometown, college or university, e-mail etc. The user can also use this list without rememberance. By this feature, a user has the higher possibility to search accurately, as the people rarely have same attributes in their personal details [14].

**3) Friend Request**

If person *X* wants to become a friend with another person *Y*, X has to send a request exploiting this feature. After receiving the request, *Y* can accept the friend request by analysing *Y*’s profile that basically includes profile picture, name, and mutual friends and so on. *Y* can reject the *X* if not interested. *Y* can investigate more information of *X* by connecting through *X*’s time-line [14].

**4) People You May Know**

This feature suggests a list of few friends that might be known based on mutual friends of user’s friend. Their features are consisted of profile picture, name, and mutual friends of friends you may know. The user can add or remove a friend from the provided list as well. It is also called as a friend recommendation system [14].

## IV. PROPOSED METHOD

In Facebook, like Social Media, people share about them and also, whatever they liked to share by means of a post, pictures, videos, comment, etc. To improve the efficiency of recommending a reliable friend, the proposed system mainly concentrates on Semantic Analysis of the text posting on Online Social Network. Based on their posts, Friend

Requested users will be grouped as Positive, Negative and Netural minded.

The proposed system mainly concentrate on blocking the Negative Minded People from the user's Friend Request Acceptance. It is very much essential to analyse the sentiments in posted text, because the informal sentences cannot give the exact meaning of the sentences as in dictionary.

The figure 1 given the detailed flow of the proposed model. The following are the modules in the proposed system that demonstrates the framework of the proposed approach: First, The Matching Factor (M) (attributes like Music, Sports, Movies, Occupation, Hometown, Education) is calculated to show a friend-to-be as "Prospect to become Friend" on Friend Request Acceptance.

Second, The Matching Factor (M) (attributes like Music, Sports, Movies, Occupation, Hometown, Education) is Calculated with the friends of friend-to-be. So, People You May Know will show the suggested friends of friend-to-be as "Propect To Become Friends".

Third, Posts posted by friend-to-be is analysed by Semantic Analysis to identify the behaviour of the people.

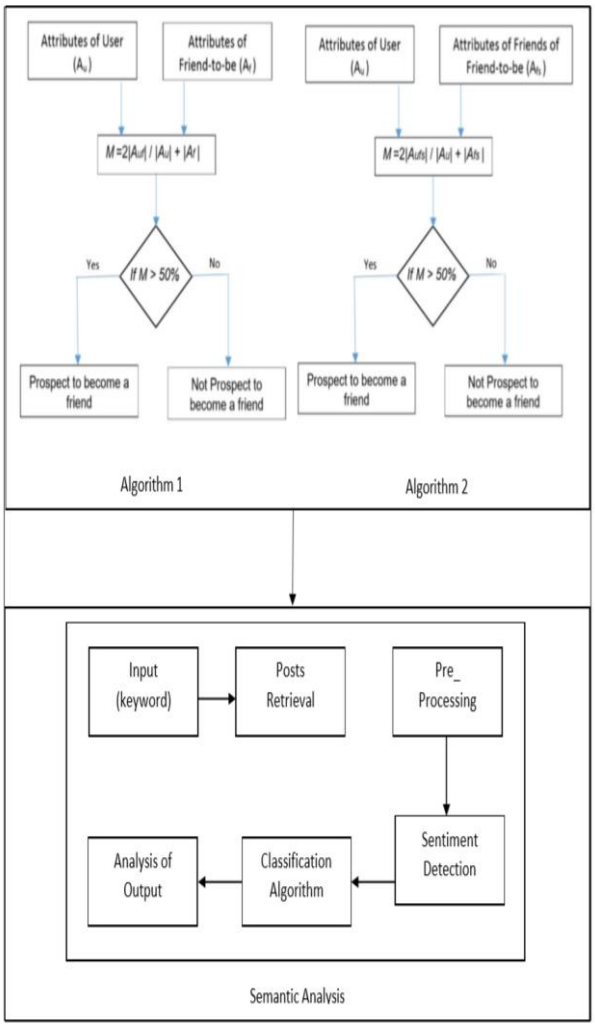



Fig 1 Proposed System Design

**ALGORITHM 1**

Step 1: From user' profile, detect his/her types of interests (correspondingly to Facebook Interest Categories, i.e. Sport, Music, Movies, Hometown, Occupation, Education, etc.).

Step 2: Declare two supersets of attributes Au and Af , which elements are sets of values of interests of a user and of a friend-to-be correspondingly.

Step 3: Define the set of common attributes Auf as an intersection of Au and Af Auf =Au∩Af.

Step 4: Define value of user' and friend-to-be' profiles matching as ratio M1 = 2|Auf| |Au|+|Af|

**ALGORITHM 2**

Step 1: Define set of waited attributes Au of a user. Assign value 1 to weight of every attribute of the set Au.

Step 2: Define set of common attributes Af s of friends of a friend-to-be.

Step 3: Define set of common attributes Auf as intersection of Au and Af s Aufs =Au∩Afs.

Step 4: Compute sum of weights of common attributes, from 1 till|Aufs| Wufs = E|Aufs| n=1 Wufs n.

Step 5: Compute sum of weights of all attributes of friends of a friend-to-be, from 1 till|Afs| Wfs = E|Afs| n=1Wfs n.

Step 6: Compute M as normalized value of weights of common attributes M = Wufs / Wfs.

**SEMANTIC ANALYSIS**

**Semantic analysis** is the task of ensuring that the declarations and statements of a program are semantically correct, i.e, that their meaning is clear and consistent with the way in which control structures and data types are supposed to be used.

In Semantic Analysis, it present a method for detecting an individual's level of conscientiousness based on an analysis of the content of the Facebook status updates. This model is based on the identification of semantic evidence of facets related to conscientiousness; an individual's belief of their control over events around them and their goal orientation.

**Raw data collection:** This consists of extracting statuses updates posted by users.

**Feature extraction:** The feature extraction is the first step to perform on collected Facebook statutes updates. It consists on reprocessing our raw data and defining the main extracted features from it.

Social network dataset consist of most noisy and unwantd data, to improve the accuracy of the input data the preprocessing has been applied. Data preprocessing consists of four steps: Pre-Processing, stop word removal, stemming and Normalization.

**Pre-Processing**

The preprocessing involves the stop word removal, stemming, normalization.

***Stop word removal***

The stop words are words that do not add meaninful content to the dataset (i.e., pronouns, prepositions, conjunctions, etc). Consequently, removing them reduces, significantly, the space of the items in the training and testing texts, and simplifies the targeted analysis.

A stop word is a commonly used word (such as "the", "a", "an", "in") that a search engine has been programmed to ignore, both when indexing entries for searching and when retrieving them as the result of a search query[15].

***Stemming***

Stemming is the process of removing prefixes and suffixes leaving the stem or the root of the considered words. The common classifiers and learning algorithms cannot handle the emotional text directly. Therefore, we have to represent them in a form that classification algorithm can deal with. The

status are typically represented by a feature vector.

Stemming is the process of conflating the variant forms of a word into a common representation, the stem. For example, the words: "presentation", "presented", "presenting" could all be reduced to a common representation "present" [15].

***Normalization***

Normalization generally refers to a series of related tasks meant to put all text on a level playing field: converting all text to the same case (upper or lower), removing punctuation, converting numbers to their word equivalents, and so on. Normalization puts all words on equal footing, and allows processing to proceed uniformly[15].

**SENTIMENTAL DETECTION**

**Lexicon developments:** This focuses on the informal language of online social networks. For this reason, three types of lexicons were created: lexicon for social acronyms, lexicon for emoticons and lexicon for interjections.

**CLASSIFICATION ALGORITHM**

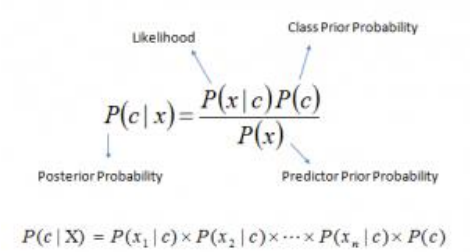
The process used to collect information and data for the purpose of accepting a friend. The methodology may include surveys and other research techniques, that includes both present and historical information. For this, Naïve Bayes Algorithm is used.

**Naïve Bayes Algorithm**

Naive Bayes classifiers are a collection of classification algorithms based on Bayes' Theorem. It is not a single algorithm but a family of algorithms where all of them share a common principle, i.e. every pair of features being classified is independent of each other.

**Bayes' Theorem**

Bayes' Theorem finds the probability of an event occurring given the probability of another event that has already occurred. Bayes' theorem is stated mathematically as the following equation:




Above,

- P(c|x) is the posterior probability of class (c, target)
- given predictor (x, attributes).
- P(c) is the prior probability of class.
- P(x|c) is the likelihood which is the probability of predictor given class.
- P(x) is the prior probability of predictor.
- Based on the data set, choose any of above discussed model. Below is the example of Gaussian model.

## VI. EXPERIMENTAL RESULT

**Data Set**

In this study, the data collected from nearly 100 Face book Account holders to know participant's responses on accepting friend request in Online Social Networks. The participants of this study are my collegues, students and known persons who have

facebook accounts, as facebook is the most prominent OSN.

The Dataset used for the implementation of the proposed system is having the following attributes: Userid, Username, Password, Firstname, Lastname, Date of birth, Contact Number, Emailid, Gender, Educational Qualification, Occupation, Hometown, Workplace, Profile Picture, Interests in Music, Movies, Sports, Fromid(communication from), Toid(delivered to), Status for request, Status for "Prospect to become a friend", Status for behaviour, Message, etc.

In addition, the attribute text posts for facebook are created and used. These posts are taken into consideration for the following simulation results. It is clearly understood that the posts are pre-processed and clustered from the given Facebook dataset for analyzing the behaviour of the user as whether they are positive minded, negative or netural.

**Performance Measure**

The performance of the proposed system is measured by using the Likert-Type scale of 4. A quantitative research has been done to study the participants' responses on accepting friend request in facebook. Measuring the acceptance or opinion of different friend request systems as 'm'. Scale 1=strongly disagree; Scale 2=disagree; Scale 3=agree and Scale 4 = strongly agree. The performance is measured in terms of Security, Flexibility, Effectiveness and Satisfaction.

**Result Analysis**

The performance analysis of the existing methods like 1) Blindly Acceptance; 2) Manual Acceptance; 3) Reliable Decision Making on Acceptance (RDM) and the proposed method namely RDM using Semantic Analysis Acceptance being used to recommend a reliable and secured friend on OSNs: is analyzed with respected to the performance measures like Security, Flexibility, Effectiveness and Satisfaction.

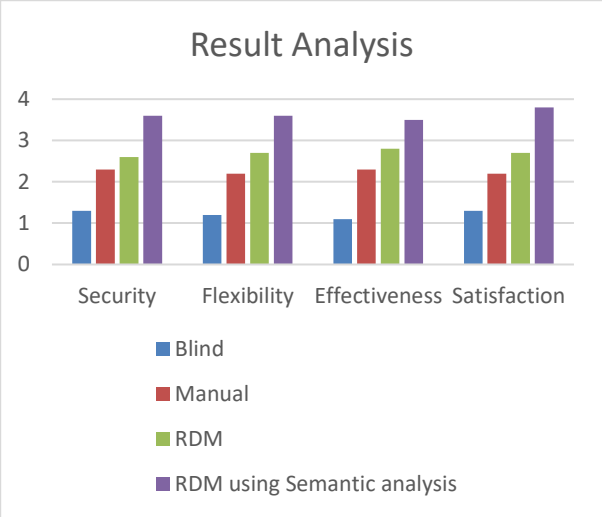



Figure 2 :Result Analysis

The above figure, reveals that the participants mostly gave their more consent on the proposed method than Blind, Manual and RDM. Since it takes less time to make friend with secured, flexible, effective and more satisfiable manner, the participants are showing positive attitude towards the proposed method on Security, Flexibility, Effectiveness and Satisfaction.

## VII. CONCLUSION

Facebook is an ever-widening Online Socical Network where users post photos, images, videos, messages, comments and etc., for all their friends to interact. In some cases, the acquisition of information cannot be restricted if the user sets their profile as

"public". Sharing information with unknown OSN user is a risk which leads to be a target by the attackers. In order to address this issue, in this research, large amounts of facebook data were collected and analysed, to find correlations in societal interactions and studied the existing FRA methods and also identified the limitations. Based on those, it is proposed to recommend a friend-to-be as a reliable and secured friend on OSNs by semantic analysis. It is designed *as an automated filtering algorithm that estimated not only a matching factor but also comparing the posts posted by the friend-to-be, with the societal behaviour and attitudes of good and bad things, which reveals the positive, negative and neutral minded people who gave a friend request*. It is very evident that the proposed method is more Reliable to recommend to accept or neglect the requests of friend-to-be in a secured manner on OSN.

## *REFERENCES*


[1] *C. Sibona and S.Walczak, ``Unfriending on Facebook: Friend request and online/offline behavior analysis," in Proc. 44th Hawaii Int. Conf. Syst. Sci. (HICSS), Kauai, HI, USA, 2011, pp. 1_10.*

[2] *B. Zhou and J. Pei, ``Preserving privacy in social networks against neighbourhood attacks," in Proc. IEEE 24th Int. Conf. Data Eng. (ICDE), Cancún, Mexico, Apr. 2008, pp. 506_515.*

[3] *C. Dwyer, S. Hiltz, and K. Passerini, ``Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," in Proc. 13th Amer. Conf. Inf. Syst. (AMCIS), Keystone, CO, USA, 2007, pp. 339_350.*

[4] *C. Zhang, J. Sun, X. Zhu, and Y. Fang, ``Privacy and security for online social networks: Challenges and opportunities," IEEE Netw., vol. 24, no. 4, pp. 13_18, Jul./Aug. 2010.*

[5] *M. Fire, R. Goldschmidt, and Y. Elovici, ``Online social networks: Threats and solutions," IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 2019_2036, 4th Quart., 2014.*

[6] *V. Sharma, I. You, and R. Kumar, ``ISMA: Intelligent sensing model for anomalies detection in cross platform OSNs with a case study on IoT," IEEE Access, vol. 5, pp. 3284_3301, 2017.*

[7] *P. W. L. Fong, M. Anwar, and Z. Zhao, ``A privacy preservation model for facebook-style social network systems," in Proc. Eur. Symp. Res. Comput. Secur., 2009, pp. 303_320.*

[8] *B. Carminati, E. Ferrari, and A. Perego, ``Enforcing access control in Web-based social networks," ACM Trans. Inf. Syst. Secur., vol. 13, no. 1, pp. 1_38, 2009.*

[9] *S.F.T. Kuan, B.FY. Wu, and W.FJ. Lee, "Finding friend groups in blogosphere," in Advanced Information Networking and Applications; Workshops, 2008. AINAW 2008. 22nd International Conference on, mar. 2008, pp. 1046 –1050.*

[10] *J. Leskovec, K. J. Lang, and M. W. Mahoney, "Empirical comparison of algorithms for network community detection," Proceedings of the 19th international conference on World wide web WWW 10, vol. 30, p. 631, 2010.*

[11] *R. Santana, C. Bielza, and P. Larraaga, "Optimizing brain networks topologies using multi objective evolutionary computation," Neuroinfor; matics, vol. 9, 2011.*

[12] *Adomavicius, G. and A. Tuzhilin, toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. Knowledge and Data Engineering, IEEE Transactions on, 2005.*

[13] *Mangina, E. and J. Kilbride, Evaluation of key phrase extraction algorithm and tiling process for a document/resource recommender within e-learning environments. Computers & Education, 2008.*

[14] *M. Fire, D. Kagan, A. Elyashar, andY. Elovici, ``Friend or foe? Fake profile identification in online social networks," Social Netw. Anal. Mining, vol. 4,no. 1, p. 194, 2014.*

[15] *C. Zhang, J. Sun, X. Zhu, and Y. Fang, ''Privacy and security for online social networks: Challenges and opportunities,'' IEEE Netw., vol.24, no.4, pp. 13–18, Jul./Aug. 2010.*


---