A Machine Learning way to Build Trust on Social Network.

ChitralaKavitha, S. Nageswararao

Abstract: ***A social network is a type of service provided by the online platform where an individual can communicate easily with each other, it also provides personal relationships and social interactions. Apart from this it also provides the website where users can build a public figure(profile) and can interact with other users. The social networking sites mainly have the trust issues to overcome, this we tried to build trust in online networks by using the Naive Bayes algorithm algorithm which is deployed through by communication direct and indirect trust and for calculating the trust values Bayesian conditional and Dempster-Shafer theory is implemented. Reenactment results with various arrange parameters are introduced to show the adequacy of the proposed plan.***

Keywords : Online social network, trust, indirect trust, Naïve Bayes

I. INTRODUCTION

The online social network basically implies any human interaction or sharing data through the web that happens through the mechanism of PC, mobile or portable. There are various sites and applications that make it conceivable. Online life is presently getting to be one of the largest way of interaction and that the reason social network plays a wide role in day –to –day life. We are living in the period and age where the data or information is just a button press and the whole data is around us that's the reason social network had a rapid growth of rate, and apart from this online network is an important factor which we can't ignore it. Nowadays online social network becomes the controversy topic today because a majority of the people think that it just destroy the human's life whereas some other people think that social network is a boon(blessing) because it connects the people from all over the world. we can say that with the help of social medium our life becomes much faster and more convenient. But as the social network also holds the trust issues one can think about is social networking is trustworthy or not? As trust plays a wide role in online social networking because trust cannot be built so easily even in reality. One must need to engage their time and commitment. Huge number of people using online social networking sites not even wait for a second to express their files, experiences, videos, images and thoughts which are links in a domain that in a great extent without any security principles and practices. People easily trust the other individuals with their way of data, character, aptitude and even with the cash loaning(money leading). Generally, users trust the social networking sites providers to keep their photos and information private with this the user might be thinking that individuals data are safe context trust.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author

Chitrala Kavitha*, CSE, Vardhaman College of Engineering, affiliated with Jawaharlal Nehru Technological University, Hyderabad, India. Email: chitralakavitha01@gmail.com

Nageswararao Sirisala, CSE, Vardhaman College of Engineering, affiliated with Jawaharlal Nehru Technological University, Hyderabad, India. Email: nagsirisala@gmail.com

A. *Trust*

A trust is a relationship between two person when they are connected to each other ,and reliable and think that they are not going to harm . in general we can say that if u trust someone we feel safe. Trusting a person always depends on ones individual behavior.

B. Types of trust in online social networks:

All though OSNS connects the one individual to all over the world but it can even mislead the information and data. In that particular situation trust plays a major role to reduce the complexity. In OSNS trust can broadly divided into two types i.e. micro and macro level.

C. Micro level phenomenon:

Micro level was established for the organization's or large industries where group of people working on it. The micro level trust is connected to altruism (goodwill) trust. It means one can be in relation with mutual understandings. And the micro level trust is a type of trust which depends on the technology and interpersonal trust.

D. Macro level phenomenon:

Macro level was established for the individual person where one person is deliberately working on it. Macro level trust is connected to legally binding trust, as legally binding trust relates to type of a agreement documents between the firms. The macro level trust is similar to math-based trust. This phenomenon depends on the benevolence (kindness), honesty, integrity, ability and competence.

E. Malicious activities on social networks:

These days, social networking is mainstream and have turned into a vital piece of our life. Many individuals are subject to OSN for different criteria. On networking sites the users perform some set of activities those activities are some times normal where as some time abnormal the abnormal one is nothing but the suspicious behavior of the user. Mainly the suspicious behavior can be term as malicious behavior. Vindictive (malicious) conduct in Online Social Networks incorporates a wide scope of dishonest exercises and activities performed by people or networks to control point of view of OSN clients to satisfy their personal stake. Such vindictive behavior need to be identify and should be reduce. By reducing we can protect billions of user by misleading information and even with security threats.

F. What exactly malicious activity is?

Malicious behavior is something to trap or spy the system or to harm the user. While speaking about social networking malicious behavior then it can be done by hacking through social sites or apps, some which come easily on mind follow:
1. Over the window: The tweets which canF. upgrade the unwanted popups.
2. Fire Foxed, which assaulted FireFox clients at whatever point they would attempt to get to the program to stole the passwords.
3. Past years all the yahoo site users affected with malware and malicious behavior.
4. Trojan assaults have influenced Facebook clients since its commencement, fooling clients into tapping on connections that contaminated their PCs with a sort of malware and constrained their Facebook records to post a comparable connection for them.
5. Even one of the attack called waterhole attack in this the clever and professional hacker can easily hack the pcs by commonly shared passwords.

Few steps to avoid malicious behavior over the online social network:

1. Must and should install Anti-virus program
2. Change the passwords on a daily basis
3. Before pressing or going throw any link take time and think twice
4. Oversharing should be avoided
5. Use a virtual private network

II. RELATED WORKS:

This part of the section deals with several trust evaluation models. The author[1] discuss that the social life impact major role in every individual life's to communicate and even to share opinions with others individual person and behind this activity, the trust plays an important role. In this paper, the author explores another trust model for an online social network. This model consists of the reputation value and interactions relations in the social network for every individual person. Apart from this, the author uses the (MF) Matrix Factorization model which is used to utilize the assess association connection between two clients. The (GKDE) Gaussian Kernel Density Estimation model is utilized to anticipate one's reputation depends on the client's other relationship. Depending upon the followers the reputation is checked and the good reputation is added and both the reputation and interaction model is combined with legitimate weights, hence from this, another model for trust is built which is used to assess the trust relationship. Author[2] say's that social Networking is practically a good way of interacting with other users who resides at various pieces throughout the country. The person can share their posts, photos, videos, etc. to the family and friends in a fraction of seconds. Yet, every beneficial thing accompanies a couple of awful perspectives also. One of the main issue in OSNs is trusting each other. So, in this paper, the author proposed a different model which mainly depends on calculating the trust based on users actions like comments, likes, messages, and shares, etc. The proposed framework orders companions as Unprivileged, Privileged and Most Trusted. These rundowns indicate the entrance level of the recorded companions to the client's asset.

The author[3] discusses that the quick pervasiveness in online social networks, the trustworthiness plays a major problem nowadays. the assessment of trust in informal organizations has been generally utilized in circumstances, for example, e-commerce, trust-based access control systems and friend recommendation. Basically to exchange the information between the users the trustworthiness is determined. And even the main objective is to recognize the trusted person in a network. The author proposes a framework that is used to calculate the node values of trust in a social network by using a reinforcement learning method. Mainly, the training feature is selected and it is checked whether there is a piece of label information at the edge in between the nodes. Next, to calculate the trust value a training model is built. And to calculate the node trust score the recommendation algorithm is used. At long last, the recreation is utilized to check the presentation of the proposed strategy. For the recreation of experimentation, information from a versatile interpersonal organization will be utilized. The author[4] in this paper bargains about the web-based business outlet, as the e-trade destinations expanding step by step, analyze the trust becomes critical to part to the client. Along these lines, in this paper, the creator presented a trust relationship through suggest frameworks and a multi-source property trust forecast technique dependent on improved D-S proof hypothesis. Whereas, right off the bat the client properties are subjectively investigated by the client singular information, and four characteristics are chosen the subjective traits is acquired from the quantitative qualities utilizing the discretization strategy. At long last, the attributes evidence is entwined again and again using the heap meeting procedure to get the trust relationship quality triple. In the generation, the sufficiency of property verification and the trust desire result are checked by the sevenfold cross-endorsement procedure. The author[5] portrays the Pervasive long range informal communication (PSN) is an important system face to face to individual correspondence that has expected basic employment on the Internet just as flexible regions. A system is required to ensure the further progression of PSN. proficient and secure correspondence is likewise a fundamental issue in PSN to build its appropriation in day by day life. In this paper, we analyze the establishment of a different leveled appraisal system to help secure and trustworthy PSN with various and variable centers. The proposed various leveled assessment framework is founded on an uncommon symmetric adjusted inadequate square plan: the (7, 3, 1)- structure and the tree structure. Together, they build up a stunning structure that supports both our different leveled trust level (HTL) evaluation system and key climb contrive. The past handles the issue of trust appraisal in PSN, and the last guarantees the protected correspondence of confided in centers. Note that both security and execution examinations show that the proposed HTL appraisal system can support expansive apportionment of capable and secure PSN.

III. SYSTEM MODEL

This section consider with the description of system , next, the Naive-Bayes model, cross-validations , Gaussian NB model presented respectively.

Retrieval Number: B4259129219 /2019©BEIESP
DOI: 10.35940/ijeat.B4259.129219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

3.1 System description:

Nowadays online social networking has rapid growth, and to pass the information they have been used the various activities. And with the help of OSNS, the user can able to manage, discover, and share their opinions and experience online. Further, the decentralized and open nature of OSNS can make them accessible to mischievous users. Therefore, prospective users face numerous issues related to trust. In this manner, efficient and effective trust assessment(evaluation) is significant for the user. With this, the user can able to understand the difference between the people who is reliable (trustworthy) and who isn't.

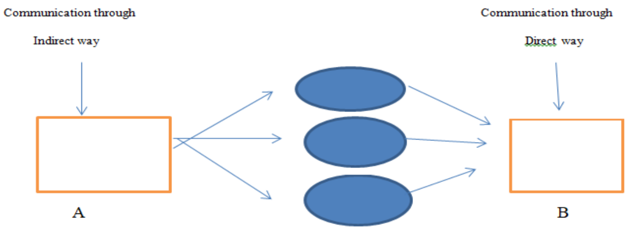

Fig 1: communicating through indirect and direct way.

3.2. Naive-Bayes model:

Naive Bayes model is a classifier where the classifier defines as an ML model that is utilized to separate various articles (objects) dependent on specific highlights (features).

Naive-Bayes model is easy to build and usually applicable for large type of datasets. and moreover it's a powerful and simple algorithm. This algorithm mainly works by two parts.

1. Naive
2. Bayes

Naive Bayes classifiers expect that the existence of an element in a class is irrelevant to some other element. Naïve Bayes mainly works on probability theory even the feature of one class is depended on other it independently contributes to all the properties. Now, let us understand the Bayes theorem.Bayes theorem is a probability and statistics theory, which describes the likelihood(probability) of an (event) occasion happening given the likelihood of another occasion that has just happened. Bayes' hypothesis is expressed scientifically as the accompanying condition:

Cross-validation: Cross-approval is a method that is utilized for the evaluation of how the consequences of statistical analysis generalize to a different data set. It is used for estimating the performance of a predictive model to get an exact accuracy. The main purpose of cross- validation is it can separate the training and testing data. Cross-approval is otherwise called revolution estimation.

Gaussian NB model: This algorithm is a special type of NB algorithm mainly used when it contains continuous values. It's additionally expected that every individual features follows the normal distribution i.e. Gaussian distribution. The Gaussian model is implemented after the competition of preprocessing. Next, the NB model is built through sklearns. With the Gaussian NB model classifier, the training data is trained. For training even we can use the fit(). once the classifier is built, the model can make the predictions, and by the predict() method test set can be determined.

3.3. Bayesian conditional trust computation in OSN(Direct Trust)

In the direct observation, the associate perceptive mobile user can be able to listen to the data or information which is forwarded by the discovered mobile user, and also analyze the discovered mobile user, mischievous behaviors, by modifying or discarding the real information or data. Even though there are multiple perceptions of the discovered mobile clients act, the associate perceptive mobile client can estimate the trust value by exploiting Bayesian inference. The Bayesian inference is one of the statistical methods of Bayes theorem which is used for the probability hypothesis update. With the Bayesian inference, we built a model by using continuous random variables which describe as Φ, and the Φ takes like 0 to 1 values. Here the Φ, follows the beta distribution i.e., Φ ~ Beta(a,b), which is defined as follows with parameters a and b

$$Beta(a,b) = \frac{\Phi^{a-1}(1-\Phi)^{b-1}}{\int_0^1 \Phi^{a-1}(1-\Phi)^{b-1}\, d\varphi}$$

Here the values of trust are assumed with two specifications i.e. a and b, and 0 ≤ φ ≤ 1

Φ is represented as a beta distribution.

We abridge our conviction of the trust Φ in a (probability distribution) likelihood dissemination iteratively as more perceptions are accessible. Expect that the earlier likelihood thickness work (prior probability density function) (pdf) at the (t−1)th perception is known. At that point, as per the Bayes hypothesis, the back circulation at the t th perception can be acquired with the pdf as

$$f_t(\varphi) = \frac{f_t\ (x_t|\Phi, y_t)\ f_{t-1}(\ \varphi)}{\int_0^1 f_t\ (x_t|\Phi, y_t)\ f_{t-1}(\ \varphi)\quad d\varphi}$$

Here, ft(xt|φ,yt) obey as a binomial distribution whereas xt and yt represent the packets of data that need to be correctly forwarded and these packets are accepted by observed mobile user at t th observation.

$$f_t(\,x_t|\Phi\,,y_t\,) = \binom{y_t}{x_t}\Phi^{\,x_t}\,(1-\Phi\,)^{\,y_t-x_t}$$

And for the binomial distribution in Bayesian deduction (inference), the beta dissemination (distribution)is the conjugate earlier likelihood conveyance (prior probability distribution). Since the probability function ft(xt|φ,yt) pursues a binomial dispersion, the prior appropriation ft−1(φ) is definitely accepted to pursue a beta circulation, which reflects what is as of now thought about the conveyance of Φ at the (t − 1)th perception.

Given that the prior appropriation ft−1(φ) pursues beta dissemination, the back dispersion ft(φ) likewise pursue a beta circulation. Especially, if ft−1(φ) ~ Beta(at−1, bt−1) and xt, yt from the tth perception is likewise given, at that point

$$f_t(\varphi) \sim \text{Beta}(a_{t-1} + x_t , b_{t-1} + y_t - x_t), t \geq 1$$

At the very first point because of no clue, distribution of Φ, stated as uniform distribution i.e., f0(φ) ~ Beta(1,1). In the same way ft(φ) pursue Beta(at,bt) with (specification)parameters.

$$a_t = a_{t-1} + x_t \quad , \quad b_t = b_{t-1} + y_t - x_t$$

$$a_0 = 1 \qquad b_0 = 1.$$

Hence, the value of trust can be expressed as mathematical expectation i.e. of beta distribution

$$\text{i.e.} \quad E_t\ [\Phi] = \frac{a_t}{a_t + b_t}$$

At the early stage, the value of trust of mobile user stands as 0.5 whereas the value gets updated according to the observations.

Now, a new factor is mentioned as a punishment factor which is used for fading reputation, because it provides the more reliable weights on mischievous behaviors in Bayesian. Here the formula for evaluation of trust as follows :

$$E_t\ [\Phi] = \frac{a_t}{a_t + Tb_t}$$

with the help of the punishment factor, the evaluation of trust becomes more reliable and realistic. It calculates the behavior in two ways the first as, if the person using mobile content any malicious behavior then the particular user check with records if it doesn't possess any bad record then the value of the trust will lower. Secondly, because of the punishment factor, the trust value quickly not recover through the behavior is not a constraint. So from the above discussion, we can evaluate the direct observation as TrD, where TrD = Et[Φ].

Trust evaluation from indirect observation:

Indirect observation also a wider role in accessing the trust for a mobile user. The indirect observation helps in criteria where one user is loyal to one person for may misbehave or cheat with another mobile user. Here, the observing mobile user will collect all the data about the mischievous user and make a decision and according to the decision the observed mobile user will be categorized whether the user is trustworthy or untrustworthy.

The Dempster-Shafer hypothesis can be utilized as a compelling method to deal with the vulnerability issue and join the proof from multiple subsidiary observers .The core of this theory is based on two thoughts: the degrees of conviction about a recommendation can be gotten from numerous abstract probabilities of a related subject, and these degrees of conviction can be consolidated together under the condition that they are from autonomous proof. In the backhanded perception(indirect observation), we accept that there are more than one backup watching portable clients and the proof given by them is commonly autonomous. And the DST outlook is collecting the evidence from particular event.

3.4. DST Function:

The DST function is based on following i.e. 1) belief function() 2) probability function() { mass function()} 3)possibility function()

Probability function:

Let X= {x1 ,x2 ,x3} is the arrangement of totally unrelated conclusion/evidences under certain contemplations. The discernment frame of X is characterized as the arrangement of all subsets of E (power set (E)) i.e.

{{∅,{x1},{x2},{x3},{x2,x3},{x1,x2},{x1,x3},{x1,x2,x3}}

The mass/ probability function (m) maps the each and every element in the range [0,1], from the discernment frame. m: P(X) → [0 1] it follows the condition like m(∅)=0 and also the

Sum of individual elements in discernment frame is 1. , i.e.

$$\sum_{b \pounds p} (X)\ m(b)=1$$

Belief Function :

For any set S in the power set, the belief function is characterized as the aggregate of mass elements of the all sets in the power set those are subsets to S. i.e.

$$\text{bel}(S) = \sum m(d)\ d \subseteq S.$$

possibility function:

For any set S in the power set, the possibility function(pl(S)) is referred as the sum of mass elements all sets in the power set those are intersect with X.

$$\text{pl}(S) = \sum m_{(\, d \cap X \neq \emptyset} \ m(D))$$

where

$$\text{pl}(S) = 1 - \text{bel}(S\overline{)}$$

Dempster's rule to be followed for combining:

let P,Q are two observer clients,their confirmations in a similar edge of decrement are mP(S), mQ(S), then the mix of these two confirmations (mP,Q(S)) is determined utilizing condition.

$$M_{PQ}(S) = \frac{\sum i \cap j = m_p(I)\, m_q(j)}{1-L}$$

Where L stands for constant which is define as

$$K = \sum i \cap j \ = \ (\emptyset)\, m_p(I)\, m_q(j)$$

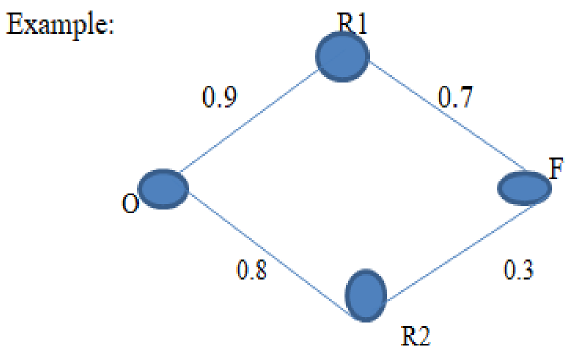

Fig2: sum of quality of service for the recommendation of trust:

In the above example the user O {R1,R2} are the adjacent neighbor's and for the F is the other adjacent neighbors. In real time the client can recommend for trust in three ways i.e. uncertainty {means distrust/trust}, distrust, trust also that it is (U={T, T̄}), such as sum(T,T̄,U) =1. The above mentioned figure illustrate the one adjacent neighbors {R!1,R2} recommendation of trust (the way as, T,¯U) for client F i.e. as {0.7,0.2,0.1} , {0.3,0.5,0.2} respectively. The client O, once received the trust recommendations, it again computes multiplying by other trust values hence it is follows :

$$m_p\,(U) = TP \times 0.1 = 0.09$$
$$m_p\,(\bar{T}) = TP \times 0.2 = 0.18$$
$$m_p\,(T) = TP \times 0.7 = 0.63$$
$$m_q\,(U) = TQ \times 0.2 = 0.16$$
$$m_q\,(\bar{T}) = TQ \times 0.5 = 0.40$$
$$m_q\,(T) = TQ \times 0.3 = 0.24$$

the above values represents TR1 and TR2 on client O opinions of trust on client R1,R2. By applying the Dempster's rule the recommendations of trust can be aggregated with mentioned trust(T) as follows

The Dempster's combine rule can be used for mix with n number of trust recommendations i.e. m1….n(T).

IV. SIMULATION:

Experiment results:

The Experiment was carried over Intel i3 processor and windows 10 platform and the experiment is implemented by deploying the python programming language .

Experiment of data:

The data set we used is Facebook performance metrics which is available public research. The data is mainly, related to posts.

The data set contains 500 of the 790 rows, Number of Instances: 500

Number of Attributes: 19

(a) The training data is consisted by 73209277 user's history concerns logs, and every log format is { Lifetime Post reach by people who like your Page; Lifetime People who have liked your Page and engaged with your post; comment; like; share; Total Interactions}.

(b) Dividing the data set into training and testing set i.e. training set 80% and testing set 20%. The experiment will completed by testing set .

(c) In this experiment, we contrast the trust through machine learning methods and once the model is build the social network direct and indirect trust samples are examined and the accuracy is compared with other methods.

Results and Analysis:

After examine the accuracy is 0.94%.

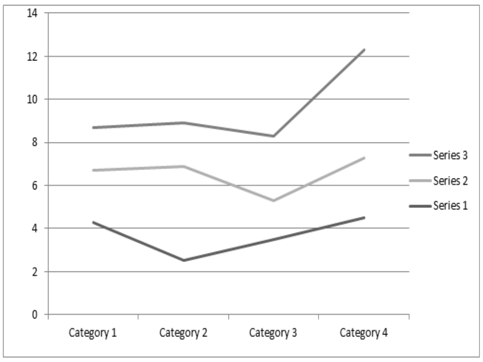

Fig 3: Direct communication v/s total interactions

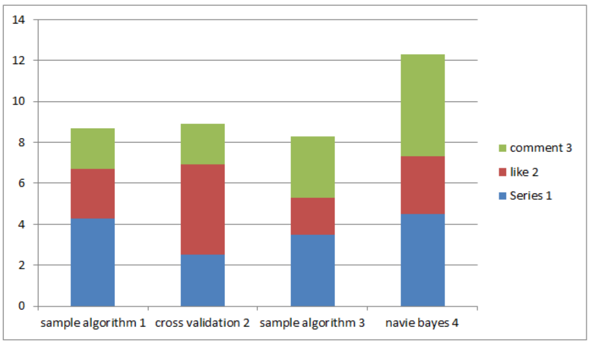

Fig 4: accuracy compared with different methods.

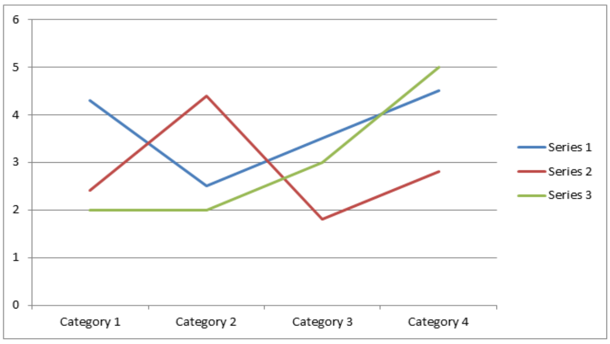

Fig 5: Indirect communication v/s total interactions

V. CONCLUSION:

The online social network is important paradigm in every individual life even in real or pratical life it plays a major role and hence the sharing data need to be secure and trustworthy. We used machine learning platform and the method is navie bayes algorithm therefore the trust can be measured by direct and indirect method by using Bayesian inference and dempster shafer theory and the result are more stable and accurate

Retrieval Number: B4259129219 /2019©BEIESP
DOI: 10.35940/ijeat.B4259.129219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

REFERENCES:

1. Wang Yuji, " The Trust Value Calculating for Social Network Based on Machine Learning": Conference on Intelligent Human-Machine Systems and Cybernetics ,USA (2017).
2. Wang Yuji ,"A Trust Prediction Method for Recommendation System", Conference on Human-Machine Systems and Cybernetics, USA(2017).
3. Yefeng Ruany, "A Survey of Trust Management Systems for Online Social Communities –Trust Modelling, Trust Inference and Attacks": Department of computer & information science ,In USA(2016).
4. Kang Zhao, and Li Pan : "A Machine Learning Based Trust Evaluation Framework for Online Social Networks" IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications 2014.
5. Pasquale De MEO, Emilio Ferrara, "Trust and Compactness in Social Network Groups" IEEE TRANSACTIONS ON CYBERNETICS 2015.
6. NageswaraRao Sirisala and C.Shoba Bindu , "A Novel Q o S Trust Computation in MANETs Using Fuzzy Petri Nets", International Journal of Intelligent Engineering and Systems, Vol.10, No.2, (2017), pp 116-125.
7. SHUIGUANG DENG, "On Deep Learning for Trust-Aware Recommendations in Social Networks", IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS(2017).
8. JIAN SHEN, "Hierarchical Trust Level Evaluation for Pervasive Social Networking", in 2017.
9. YADONG ZHOU1 , DAE WOOK KIM2, JUNJIE ZHANG2," Pro Guard: Detecting Malicious Accounts in Social-Network-Based Online Promotions", ON TRUST MANAGEMENT IN PERVASIVE SOCIAL NETWORKING,2017.
10. Vu Viet Hoang Pham : "Privacy issues in social networks and analysis: a comprehensive survey" Security Architecture and Technologies for 5G ,in 22nd October 2017.

AUTHORS PROFILE

Chitrala Kavitha, currently pursuing M.Tech final year in Vardhaman College of Engineering, completed graduation in B.Tech from Vidya jyothi Institute of Technology, Hyderabad in the year 2017. A paper published in the year 2019 journal named as International Journal of Computer Science and Engineering.The title of the paper "A survey on Trust Computation in Online Social Network". Area of interest is Machine Learning.

Dr. NageswaraRao Sirisala, working as an Associate Professor in Vardhaman College of Engineering, Hyderabad. He has 14 years of Experience in teaching and research. He received PhD in the Dept of Computer Science and Engineering (CSE), from JNT University Anantapuramu, AP, India. He completed M.Tech (Computer Science and Engineering) in Pondicherry Enigeering College, Puducherry and B.Tech (Computer Science and Engineering) from JNTUH Hyderabad. He has published more than 20 research papers in international conferences and journals. His area of interest is computer networks, Mobile adhoc networks, algorithms, soft computing methods, distributed systems, mathematical foundation of computer science, designing of data base and programming languages

Retrieval Number: B4259129219 /2019©BEIESP
DOI: 10.35940/ijeat.B4259.129219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication