International Journal of Research in Advent Technology, Vol.7, No.5, May 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

A Neuro-Fuzzy based Inconsistency Location Display to Represent Efficient Recognition in Social Networks

Sahena Rameez[1], D Manju[2]
PG Scholar, Dept. of CSE,GNITS.Hyderabad, India. Email[1]:sahena121294@gmail.com
Asst.Professor, Dept. of CSE, GNITS Hyderabad, India. Email[2:] s.r.manju55555@gmail.com

Abstract- Utilization of an informal organization is the fundamental usefulness of the present life. With the number of online web based networks increases day by day, the data accessible and its usage have gone under the risk of a few inconsistencies. Abnormalities are the significant reason for online fakes which permit data access by unapproved clients just as data producing. One of the abnormalities that go about as a quiet aggressor is the flat peculiarity. These are the abnormalities brought about by a client on account of his/her variable conduct towards various sources. In this paper, a self-recuperating neuro-fuzzy methodology is utilized for the discovery, reoperation, and expulsion of level inconsistencies efficiently and precisely. This methodology works over five methods, particularly, missing connections, notoriety gain, significant distinction, property trust, and score trust. I have assessed with the NHAD [1] model with DARPA'98 benchmark dataset. Results demonstrates the exactness of model displayed 10% to 30% peculiarities in manufactured dataset goes somewhere in the range of 98.08% and 99.88%. The assessment over DARPA'98 dataset shows that the methodology is superior to the current arrangements as it gives 99.97% identification rate to strange class.

Keywords- Horizontal Anomaly, Social Networks, Reputation, Neuro-Fuzzy Model.

1 INTRODUCTION

Online interpersonal organizations permit efficient communication between the clients and the data sources. With the approach of progressively online internet based life, controlling the data has turned into a noteworthy test. One of these methods includes identification of system abnormalities and exceptions. Oddities are the sudden conduct of the client which results in sporadic and suspicious action which makes the data dangerous [2] [3]. In view of the system, these peculiarities enable client data to be recovered without consent and use it against the ability of online network. Peculiarities are classified into static named, static unlabeled, powerful marked and dynamic unlabeled [4] [5]. Abnormality discovery can be performed in various distinctive ways: classification, grouping, phantom investigation, data theoretic, closest neighbour and measurable strategies [6] [7] [8]. With the appearance of expanded online social association destinations, client following and inconsistency recognition in informal organizations are two of the real zones of research. The essential objective of distinguishing irregularities is to recognize the patterns of various exercises in the system. A ton of research has been done to manufacture a summed up method for anomaly detection. A number of well-created techniques are accessible for recognizing them under specific conditions on various areas. A standout amongst the most threatful inconsistencies predominant in the online interpersonal organization is the flat abnormality. Even irregularity is unique in relation to static and dynamic classification and has a place with the conduct classification of social abnormalities. It alludes to the distinction in the connection conduct of the client dependent on the clients' specific movement in a network over the online informal community. Flat peculiarity is difficult to follow and distinguish as it totally relies upon the distinctive sources collaborated by a client. A client may experience specific conduct towards a specific source which could possibly be treated as a peculiarity. Therefore, it ends up most extreme essential to characterize the total framework which can promptly distinguish the suspicious conduct and can resolve these irregularities. In the course of the most recent couple of years, discovery of the oddities has been taken as a genuine research which required efficient approaches for improved identification. Therefore, the methodologies given so far are legitimate for systems under certain pre-defined parameters which for the most part includes the dimension of data trade between the source and the clients. Further, there is no architecture of the parameters which can be used for the location of level irregularities.

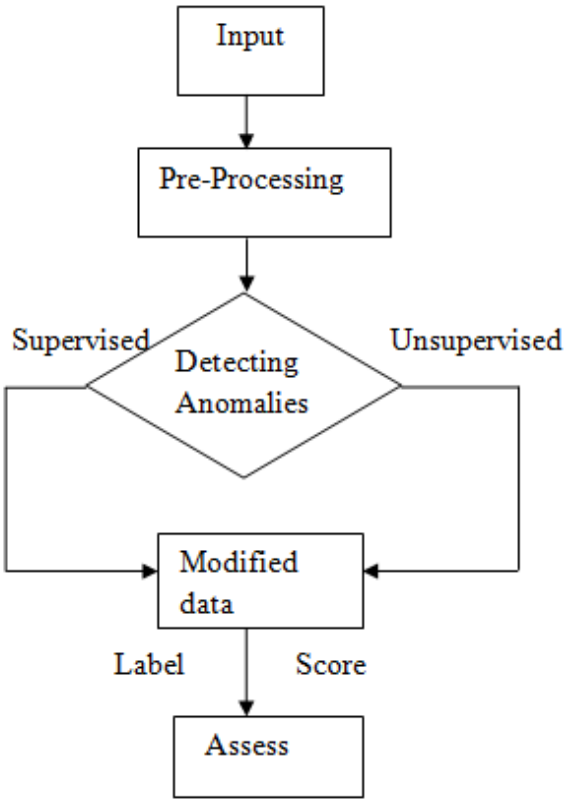

Fig. 1: Framework for Anomaly Detection in Networks.

The current arrangements can resolve the abnormalities utilizing the system action instead of the clients' methodology towards a specific source. Assessments performed based on system action can give wrong outcomes as clients' system action can be purposeful, while the clients' constant connection with a specific source can give more insights regarding its conduct in online informal communities. The Figure 1 shows a generic framework for network anomaly detection. The input data needs pre-processing because the input data is in many forms, for example, as we know the protocols used are categorical in nature, whereas IP addresses are hierarchical and port numbers are numerical.

Pre-processing techniques are based on the different anomaly detection techniques. The techniques of anomaly detection are classified into supervised and unsupervised approach and are applied on the pre-processing data. For assessing the modified data, either labels or scores are used. As network anomaly detection is very difficult to detect, ensure to find the data that do not follow normal behavioral patterns.

1.1 Motivation

Efficient strategies are required which not only target the identification of even peculiarity as an issue yet ought to be fit for recuperating the entire system efficiently with high accuracy. Thus, the objective of this paper incorporate the identification of flat irregularities, reoperation of clients and disposal of non-recoverable clients devouring less cycles with lower mistakes, higher precision, and less disappointments. In this paper, a neuro-fuzzy based flat irregularity location demonstrates the permits discovery, reoperation, and evacuation of level abnormalities efficiently and accurately. The model operates over five methods, particularly: missing connections, notoriety gain, significant distinction, properties trust, and score trust. The model structures the trust-based notoriety chart. At that point, it constructs oneself mending neural model dependent on its trust properties. Next, it utilizes the fuzzy framework to finalize the final cost, in view of which a choice is made within the sight of the oddity. The model permits efficient and precise recognition of flat abnormalities in online interpersonal organizations.

2 LITERATURE SURVEY

The abnormality recognition in online interpersonal organizations can be completed in various ways. Throughout the years, numerous variants of anomalies have been identified and targeted with key arrangements. These arrangements center around the order of the peculiarity and further gives arrangements which can resolve the issue of client identification.

2.1 Guideline based Anomaly Detection

Defining the rules for collaboration can help in identification of oddities. Akoglu et al [9] considered the inconsistencies in the weighted charts and built up an Oddball calculation for finding the influenced hubs. They used the rule based way to deal with these abnormalities. The methodologies are equipped for recognizing a specific abnormality in a constrained situation. These methodologies are not ready to distinguish hub conduct in online interpersonal organizations as these depend just on the associations between the hubs, which can be controlled effectively. This control can be the consequence of various properties for various associations.

2.2 Vehicular and Crowd Anomaly Detection

The dimension of irregularities can influence the utility of the informal organization and this has been contemplated as the vehicular inconsistencies by Giridhar et al [10] under the name of ClariSense+. They proposed an augmentation to the irregularity clarification framework and tried their methodology in the vehicular condition. Their methodology centers around the sensor capacities of the system and identifies the issues with the event of the abnormalities in the comparable condition. Chaker et al [11] considered the group inconsistency discovery and limitation in both nearby and worldwide informal communities. Picturesque elements are utilized by them to distinguish the group oddity with higher exactness.

2.3 Collaboration based Anomaly Detection

Purpose of collaboration can be another answer for distinguishing abnormalities. Such methooldogy uses the idea of peculiarity scores by breaking down the sources with a client. Takahashi [12] proposed change-point recognition method which utilizes the Sequentially Discounting Normalized Maximum Likelihood. They used the peculiarity scores acquired from these investigations to distinguish the connection irregularities. In the other methodology by Yu et al [13], they proposed a Group Latent Anomaly Detection

approach which uses the pair-wise as well as point wise information to deduction at the final choice of irregularities. Their methodology is efficient yet needs relevance to the level oddities in light of its reliance on gathering highlights for every person, even though irregularities a rise due to an individual's activity irrespective of the group to which it has a place.

2.4 Traded off Account-based Anomaly Detection

Another part of the irregularities in the online informal organizations is the bargained records which have been analyzed by Egele et al [14] [15]. They built up a methodology under the name of Traded off account-based anomaly detection, which can recognize the records in the greater part of the person to person communication locales. They broke down and tried the methodology on an expansive informational index involving around 1.4 billion Twitter messages which are publicly available. These systems can be classified as Intrusion Detection Systems especially concentrating on the abnormality discovery in the online social networks as stated by Sommer and Paxson [16]. The authors displayed the utility of Artificial Intelligence ways to deal with the arrangement of an Intrusion Detection Systems which can efficiently follow the system inconsistencies. These abnormalities are constrained to the social records, yet these can likewise make impacts on the systems working these pernicious sources. Zhu et al.[17] considered the similar aspect of the anomalies in the cellular systems. The authors used the web based life traffic and the telephone information for worm regulation in cell systems. Identification of traded off records is one of the real difficulties and the above methodologies are appropriate. Therefore, these methodologies can be utilized after an assault. Artificial intelligence components are efficient, yet in the above cases, a pre-noteworthy preparing of the recognition framework is required, which can be kept away from by an abnormal hub.

In figure 2, Categories of Anomaly are divided into five types such as; point, group, conditional, insertion, modification and deletion anomalies. In addition, it gives the types of attacks that occurs in the network. Each type of attack has specific behavior.

2.5 Point Anomaly

When a given particular data instance changes from the normal pattern of the dataset, it is said to be a point anomaly. The attacks that occur in point anomaly are remote to local and user to root.

2.6 Group Anomaly

When in a collection of similar data instance behaves anomalous when compared to the entire dataset, then this collection of data is called group anomaly. The attacks that occur in group anomaly are Denial of Service and Distributed Denial of Service.

2.7 Conditional Anomaly

When a given data instance behaves anomalous in a particular context, but not in other context, then it is called conditional anomaly. The attack that occurs in conditional anomaly is probe.

Further, in the normalization of database, insertion anomaly occurs when the user wants to add new rows to create duplicate data. The modification anomaly occurs when the user wants to change already existing records. The deletion anomaly occurs when the user wants to remove the records.

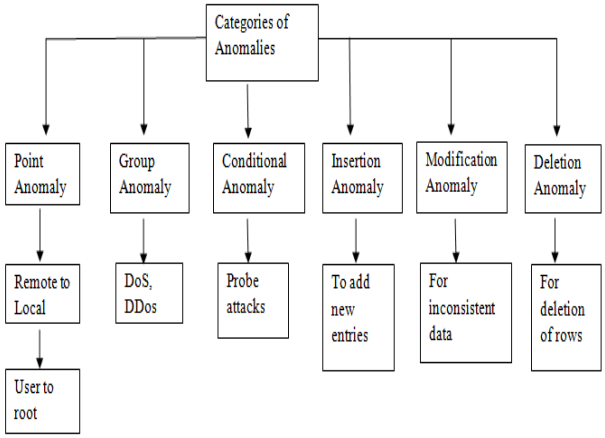

Fig. 2: Categories of Anomalies

2.8 Factual Anomaly Detection

Insights can be another answer for the issues identified with the oddity identification. Utilizing the idea of measurements, Heard et al [18] proposed an efficient framework for irregularity discovery in the interpersonal organizations, which especially utilizes the Bayesian examination approach. A two-stage approach is utilized by the authors for the irregularity discovery which decreases the gathering of conceivably bizarre hubs. The current arrangements depend much on the gathered information, which can be utilized just on account of educated oddities. In any case, real time identification, checking and cautioning frameworks are excluded in the current methodologies, which are required for the arrangement of an efficient framework for identifying level abnormalities. Past work displayed in this segment obviously demonstrates that the greater part of the current methodologies have been conventional in the discovery of the inconsistencies and have not thought about the flat irregularities. In this manner, efficient approaches are required which cannot just distinguish the danger level brought about by those irregularities yet additionally settle these efficiently.

3 EXISTING SYSTEM

The current arrangements can resolve the inconsistencies utilizing the system action as opposed to the clients' methodology towards a specific source. Assessments performed based on system action can give mistaken outcomes as clients' system movement can be deliberate or accidental, while the clients' ceaseless association with a specific source can give more insights regarding its conduct in online interpersonal organizations. Arrangements like Communication Processing Architecture for Wireless Sensor Networks [19] and Bayesian [18] oddity identification are accessible for the location of peculiarities in online informal communities. The Bayesian methodology uses the Bayesian separating

component to recognize the strange hub in the interpersonal organization, while Communication Processing Architecture for Wireless Sensor Networks manages the distinguishing proof of the covering networks in the informal communities. Communication Processing Architecture for Wireless Sensor Networks can be utilized to distinguish irregularities by deciding the clients in the non-covering networks. Despite the fact that these methodologies are successful, they are unfit to give reoperation. Existing neuro-fluffy methodologies like Mobile Fuzzy Trust Inference [21], Modularity expansion [22] and Hybrid Genetic Detection [23] can likewise be reached out for identifying diverse clients in a given informal organization. At present, these methodologies are assessed for recognizing trust between two clients and for network discovery. On a more extensive form, these methodologies can be coordinated with inconsistency recognition instrument and their current correspondence grouping can be utilized for distinguishing flat abnormalities. In any case, this may build the multifaceted nature of the general framework. Some different arrangements incorporate co-bunching based aggregate abnormality discovery utilizing system examples, and self-learning interruption recognition frameworks [24] that utilization Radial Basis Functions neural system to determine inconsistencies. Likewise, there are numerous methodologies that essentially center around sending Support Vector Machine [25] alongside different belief systems to identify strange conduct. A portion of these are inconsistency discovery with chief part investigation and Support Vector Machine, self-sufficient marking with Support Vector Machine, and troupe procedure for abnormality recognition which utilizes Support Vector Machine in blend with the Extended Kalman Filter. Despite the fact that, the execution consequences of these arrangements over standard benchmarks recommend their effectiveness, yet these don't contain suitable highlights of online informal organizations which are required for the identification of level irregularities

4 METHODOLOGY

The given model goes for marking a specific client in a network of an online interpersonal organization to be a peculiarity or not. The model utilizes the current self-recuperating neural model for instating the oddity distinguished as a spurious neuron in the neural setup of the networks of an online informal organization. At that point, this neural model recuperates utilizing a fuzzy derivation framework with conceivable outcomes of recouping a client before totally annihilating it. The notoriety increase of every client goes about as a weight, and a mending cost is registered for every one of the clients. This recuperating cost is then used to locate the ultimate result for a hub's action; for example either an inconsistency or an authentic client. For recuperating model application, the model is sorted as the neural setup. The neural setup represents the m number of clients in the jth network each treated as an information neuron with weight identical to their notoriety gain. The shrouded layer is framed from the sources dependent on the client action. The yield of the neural model creates an edge cost beneath which the client is treated as a peculiarity. The last expense of a client is determined after De-fuzzification of the fuzzy set over Tp.

4.1 Objectives

• A quicker union methodology in spite of the quantity of abnormalities, less emphases to stamp a client as an oddity and littler impact on the system movement. Further, the model indicates improvement in the intermingling cost and the exactness in the discovery of a flat peculiarity.

•Neuro-fuzzy answers for the distinguishing proof of peculiarities and framework learning.

• Recovery after identification of even oddities.

5 ARCHITECTURE

The methodology in Fig. 3, frames the notoriety chart and it utilizes the fuzzy framework to assess every client over the thought about properties for their exercises in an informal organization. Next, this notoriety diagram is utilized to locate oneself recuperating cost of every client. Following this, the edge recuperating cost, singular expense and fresh results of every client are utilized to locate the last neuro-fuzzy cost, which is utilized to choose whether a client is a threat or not.

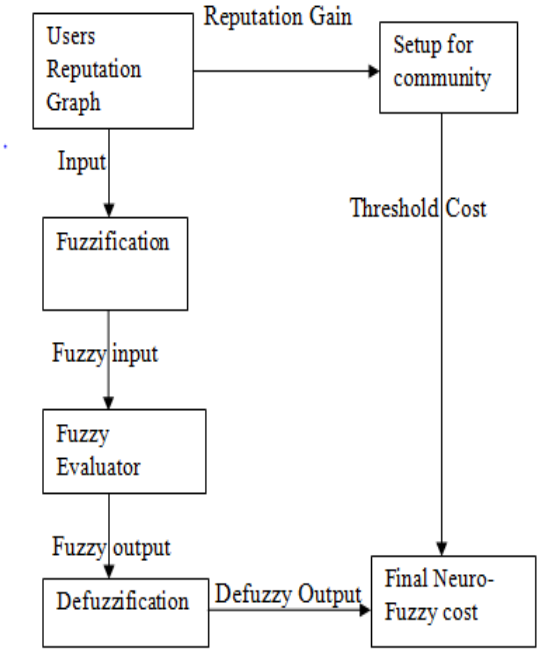

Fig. 3: Flow Chart for Detection of Horizontal Anomaly.

5.1 Mending Cost and Neuro-Fuzzy Formations

The initial phase in the model is to delineate characterized set of properties to the neural system which works by utilizing a mending cost. The mapped system is then worked on the fuzzy induction principles to produce the fuzzy sets for the conduct of every hub, which is then assessed to touch base at a choice of proclaiming a hub as a peculiarity or not.

5.2 Huge Difference

It depends on the example of collaboration between the two elements, and it helps in distinguishing proof of a client as an oddity. Noteworthy contrast controls the clients' notoriety increase and its movement over the web based life. The noteworthy contrast is greatly influenced by the client movement over unconfirmed sources. In this paper, the standardized controlling edge deviation of a client in a network is fixed at an edge of 0.5. This esteem is fixed thinking about that at the most a system can have half peculiarities. In spite of the fact that in a genuine system, this esteem is exceptionally low, yet to demonstrate the viability of the methodology, a higher abnormality rate is picked.

5.3 Notoriety Gain

Notoriety gain Rg is processed over a chart G with the end goal that G = (Tp; Ts), where Tp means the arrangement of property trust that structures the vertices of the diagram, and Ts is the arrangement of score trust allocated as weight to the edges interfacing the vertices to a specific client.

6 ALGORITHM

In comparison with other detecting algorithms in networks NHAD[1] model gives an algorithm for detecting horizontal anomalies in online social networks by giving a Neuro-Fuzzy based Inconsistency location display to represent efficient recognition.

1. Input m, n, T_p
2. Built Reputation graph based on T_p
3. Calculate Reputation Gain R_g for the users
4. Calculate Threshold Self-healing Cost S_f^{TH}
5. Calculate upper individual self-healing cost for user S_f^U
6. Initialize Fuzzy inference system
7. Compute $C_{g,crisp}$
8. $S_{f,final} = S_f * C_{g,crisp}$
9. if$((S_{f,final} > S_f^{TH}) \&\& (S_f > 0.5, S_{f,final} > 0.5))$ then
10. Declare user as an anomaly and eliminate
11. else if $((S_{f,final} > S_f^{TH}) \&\& (S_f <= 0.5, (S_{f,final} <= 0.5))$ then
12. Perform self healing and warn the user
13. Eliminate user if warning ignored (three times)
14. else
15. save R_g, reset
16. end if
17. continue detection

7 RESULTS

The results in the Table 1 gives the output for the neuro-fuzzy anomaly detection techniques, score gives an anomaly decimal value to each data instance. With the help of threshold cost, scores are given few ranks and admin selects the anomalies to them. The data instances are represented as a, b, c, d, e and anomaly scores for each instance are in between 0 to 1. In the column label, outputs are shown in a binary manner, i.e., either anomalous or normal.

TABLE 1

Data Instance	Score	Label
A	0.4	Normal
B	0.9	Anomaly
C	1	Anomaly
D	0.2	Normal
E	0.7	Anomaly

The results in the Table 2 are taken from [8] in order to compare one anomaly detection technique with other. The output gives label and score for each data instance, attack preferences are DoS, R2L, U2R and computational complexity is quadratic, linear and exponential in nature. The anomaly detection techniques which have label as an output are more systematic than the outputs which have score. In this case, information theory and clustering based anomaly detection techniques are better when compared to the classification and statistical techniques. When the priority of attack detection is concerned, the clustering-based and classification techniques are used to identify DoS attacks. Based on the computational complexity, statistical techniques are better than other techniques due to their linear complexity nature.

TABLE 2

Technique	Output	Attack Priority	Comp -lexity
Classification	Label, Score	DoS	Quadratic
Statistical	Label, Score	R2L, U2R	Linear
Clustering	Label	DoS	Quadratic
Information Theory	Label	Neutral	Expon -ential

8 CONCLUSION

In this paper, a neuro-fuzzy based flat inconsistency location display is recommended that represents efficient recognition of even abnormalities in online social networks. The given model uses self-recuperating neural model to demonstrate a fuzzy derivation framework with the likelihood of recuperating a client before removing it. The methodology is assessed by using a DARPA'98 dataset as utilized by the majority of the double classification arrangements. The mending cost technique of the model show permitted recognition, recuperation and evacuation choices in less phases, along these lines, making it an efficient conspire for the discovery of even abnormalities in online interpersonal organizations. The methodology utilizes restricted

plans notwithstanding for distinguishing complex flat abnormalities and the quantity of cycles required for touching base at a choice is not exactly the hypothetical qualities. Further, the mapping of the property trust into the final yield should be possible in a steady time. Therefore, the main multifaceted nature included is the underlying mapping of fuzzy standards and required yield. Currently, these depend on experimental assessments yet can be learning over oneself recuperating neural model. Another real favorable position is in the center proposition of the methodology, which is dependent upon the efficient recuperation component of its base neural model. With less cycle to settle, the neural model backings efficient union of the methodology. The examination in the paper demonstrates that the methodology can be utilized as an offline approach for recognizing peculiarities out of dataset just as an online methodology for distinguishing irregularities at the ongoing. Results recommend that the model turns out to be efficient as far as significant increases accomplished in correlation with the current methodologies over different parameters to be specific, peculiarity filtering rate, precision in oddity identification, combination esteem, approach disappointments, and the level of clients recouped in spite of being an irregularity.

REFERENCES

[1] Vishal Sharma, Ravinder Kumar, Wen-Huang Cheng, Mohammed A tiquzzama, Kathiravan Srinivasan, and Albert Y. Zomaya, Fellow, "NHAD: Neuro-Fuzzy Based Horizontal Anomaly Detection in Online Social Networks", IEEE Transactions, 2018.

[2] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection for discrete sequences: A survey," IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 5, pp. 823–839, 2012.

[3] Y. Park, C. Priebe, D. Marchette, and A. Youssef, "Anomaly detection using scan statistics on time series hypergraphs," in Link Analysis, Counterterrorism and Security (LACTS) Conference, p. 9,2009.

[4] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM computing surveys (CSUR), vol. 41, no. 3, pp. 15–58, 2009.

[5] C. Moore, A. Clauset, and M. Newman, "Statistical inference for detecting structures and anomalies in networks," tech. rep., DTIC Document, 2015.

[6] D. Savage, X. Zhang, X. Yu, P. Chou, and Q. Wang, "Anomaly detection in online social networks," Social Networks, vol. 39, pp. 62–70, 2014.

[7] Y. Liu and S. Chawla, "Social media anomaly detection: Challenges and solutions," in Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 2317–2318, 2015.

[8] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," Journal of Network and Computer Applications, vol. 60, pp. 19–31, 2016.

[9] L. Akoglu, M. McGlohon, and C. Faloutsos, "Oddball: Spotting anomalies in weighted graphs," in Pacific-Asia Conference on Knowledge Discovery and Data Mining, pp. 410–421, 2010.

[10] P. Giridhar, M. T. Amin, T. Abdelzaher, D. Wang, L. Kaplan, J. George, and R. Ganti, "Clarisense+: An enhanced traffic anomaly explanation service using social network feeds," Pervasive and Mobile Computing, vol. 41, pp. 381–396, 2016.

[11] R. Chaker, Z. Al Aghbari, and I. N. Junejo, "Social network model for crowd anomaly detection and localization," Pattern Recognition, vol. 61, pp. 266–281, 2017.

[12] T. Takahashi, R. Tomioka, and K. Yamanishi, "Discovering emerging topics in social streams via link anomaly detection," in 2011, IEEE 11th International Conference on Data Mining, pp. 1230–1235, 2011.

[13] R. Yu, X. He, and Y. Liu, "Glad: group anomaly detection in social media analysis," ACM Transactions on Knowledge Discovery from Data, vol. 10, no. 2, pp. 18–22, 2015.

[14] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "Compa: Detecting compromised accounts on social networks.," in NDSS, 2013.

[15] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "Towards detecting compromised accounts on social networks," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 4, pp. 447 – 460, 2015.

[16] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in 2010, IEEE. Symposium on Security and Privacy, pp. 305–316, May 2010.

[17] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci, "A social network based patching scheme for worm containment in cellular networks," in Handbook of Optimization in Complex Networks, pp. 505–533, Springer, 2012.

[18] N. A. Heard, D. J. Weston, K. Platanioti, D. J. Hand, et al., "Bayesian anomaly detection methods for social networks," The Annals of Applied Statistics, vol. 4, no. 2, pp. 645–662, 2010.

[19] S. Gregory, "Finding overlapping communities in networks by label propagation," New Journal of Physics, vol. 12, no. 10, pp. 1–26, 2010.

[20] F. Hao, G. Min, M. Lin, C. Luo, and L. T. Yang, "Mobifuzzytrust: an efficient fuzzy trust inference mechanism in mobile social networks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 11, pp. 2944–2955, 2014.

[21] J. Su and T. C. Havens, "Quadratic program-based modularity maximization for fuzzy

community detection in social networks," IEEE Transactions on Fuzzy Systems, vol. 23, no. 5, pp. 1356–1371, 2015.

[22] J. Su and T. C. Havens, "Fuzzy community detection in social networks using a genetic algortihm," in Fuzzy Systems (FUZZIEEE), 2014 IEEE International Conference on, pp. 2039–2046, 2014.

[23] N. A. Elfeshawy and O. S. Faragallah, "Divided two-part adaptive intrusion detection system," Wireless networks, vol. 19, no. 3, pp. 301–321, 2013.

[24] L. Zhanchun, L. Zhitang, and L. Bin, "Anomaly detection system based on principal component analysis and support vector machine," WuHan University Journal of Natural Sciences, vol. 11, no. 6, pp. 1769–1772, 2006.

About Authors:

1. Sahena Rameez is currently pursuing her M.Tech in Department of Computer Science and Engineering, G Narayanamma Institute of Technology and Science, Hyderabad, Telangana. I have pursued my B.Tech in CSE from Muffakham Jah college of Engineering Technology, Hyderabad.

2. D. Manju is currently working as Asst. Professor in Department of Computer Science and Engineering , G Narayanamma Institute of Technology and Science, Hyderabad. Her research interest includes Image processing, Artificial Intelligence and Data mining.