Cluster-Based Trust Model for Online Reputation System

A.Deepthi Priyanka[1], Punugoti Srikanth[2], Janapati Venkata Krishna[3]

[1]pursuing M.Tech (CSE) , [2] Assistant Professor (CSE Department) , [3] Associate Professor & HOD (CSE Department)

[1,2,3]Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India

***Abstract*- with the rapid development of online reputation systems, Manipulations against such systems are evolving quickly. In This paper, we propose a Cluster based approached theory to protect reputations. Tested against users attack data taken from a cyber-competition, the proposed system has achieved a better performance in terms of accurately identifying unwanted users. It also describes a great conceivable to effectively remove dishonest ratings and keep the online reputation system a secure and fair marketplace. We collect all the information of the user and depend on their rating we get the dishonest users. Cluster based approach means we make the clusters of different types of user on their rating status which are given by the users for different items and make all the security for his/her rating or feedback.**

***Keywords*— Clusters, Reputations, Security.**

I. INTRODUCTION

Online reputation allows users to form an expectation based on the judgements of others, It can encourage good behaviour, as user seek good reputation and getting benefit from it. Trust and reputation are strongly related, reputation enables a trust. Reputation expresses the collective opinion, leading to trust that emerges opinions of a group of members.

There is in fact a significant economic benefit in beaning able to trust strange people Opinions we use to build trust in strangers often come from other people you don't know personally since online contacts while this makes reputation like something unreliable. In reality the majority of people providing reputation feedback truthfully, there is a proof to suggest that under the right condition, group decision making can arrive good quality results. Reputation in the world is used to forecast the actions of a person hence lowering the risk involved in the trust decision.

The existing defense mechanisms protect reputation systems from different ways. First, restrict the maximum number of reputations each user could provide within certain time span. Second, growing the cost of achieve multiple user IDs by binding identity with IP address [2] or using network coordinates to detect Sybil attacks [3]. Third, investigating rating distributions through statistical techniques, such as beta-function based approach [4], entropy based scheme[5], and Bayesian model based method [6]. Fourth, investigating users' rating behaviors by building user trust, such as a personalized trust model [7], an iteration refinement approach [8] which evaluates a user's "judging power" as the inverse of this user's rating variance. The existing defense mechanisms protect reputation systems from several angles.
Limit the maximum number of ratings each user could provide within a certain time duration.

II. PROPOSED WORK

Based on the anomaly detection results, we further evaluate users' trust values in this part. Users trust values in trust models are determined only by their bad behaviors and good behaviors. But it is not enough. Consider both trust scenarios. First, user *One* has participated 5 good behaviors and 5 bad behaviors. Second, user *B\Two* is a new coming user and has no behavior history. So we give the preferences to the new one on the basis of Cluster-based. The proposed detector is used to (a) detect whether changes occur in the ratings of an item.
Estimate the time when attacks are suspected (i.e. which rating is suspicious).

With Proposed system we used the Cluster based algorithm for getting the data rating which are given by the user at specific times for the items columns. In this proposed system we are using, Partitioning Relocation Clustering algorithm. In this clustering algorithm we organise the ratings to a particular item in a descending order according to the time which was given by the user. Generally in practical reputation systems, items have stable quality, which should be effected on the distribution of item ratings. Rapid changes can serve as anomaly indicators, anomaly detectors which detects the changes on the rating of a particular online item. In this section we survey data partitioning algorithms, which divide data into multiple subsets. Because checking all possible subset systems are complex, certain greedy techniques are used in the form of iterative. Specifically, different relocation schemes that iteratively reassign points between the k clusters. Unlike normal methods, in which after construction of clusters, they are not revisited again, relocation algorithms improve clusters with certain data, this results in quality clusters.

Based on the results of anomaly detection, we evaluate the trust values of the user, generally in trust models, the trust values of the user determined by their bad and good behaviours only, but this is not sufficient to consider two trust scenarios. First, user A has 5 good and 5 bad behaviours. Second, User B is a new user and having no behaviour history, In many trust models their trust values will be calculated like 0.5 and even we are confident in the trust value of user A. To differentiate these two cases we are using cluster-based model to group the individual user's reputation values. For example two events g and b taken as a consideration where g is good behaviour and b is a bad behaviour, and here the thing is observe to perform good behaviour for *p* times and bad behaviour for *q* times

$$A_g = \frac{p}{p+q+2}$$
$$A_b = \frac{q}{q+p+2}$$

Where A_g is representing that the person will perform good behaviour and A_b is representing that the person will perform bad behaviour.

We can determine which ratings are suspicious for each given item based on the anomaly detector, then we can define a user's behaviour value on a single item to indicate whether the person's behaviour is good or bad. When user U*i* provides a rating to item I*j*, if the particular persons rating is suspicious the behaviour value of the user U*i* for item I*j* is set to 0 otherwise I*j* is set to 1. Assume that U*i* user has rated $p + q$ items the behaviour value for *p* items are 1 and *q* items are 0, suppose the user U*i* rated N items in total, except the I*j* item, The user U*i* has behaviour as 1 on *p* items and behaviour value as 0 on *q* items. The user U*i* trust value on item I*j*, which indicates that how much we could belief the rating given by the user U*i* to the item I*j*. Finally we can identify the malicious users with low trust values on the items, other than removing of all ratings provided by user we are only remove some of the ratings which are having low trust ratings for user U*i*, if T*ui* (*j*) < T*h*, The user U*i* 's rating to I*j* item is removed from the all ratings and U*i* is marked as low trust user or malicious user. T*h* is the trust value, which could be adjusted according to the different scenarios.

III. Results

To test the performance of the proposed scheme, we gathered real user attack data against online reputation systems, it is successfully collected 75% of the valid submissions from registered users, we group the malicious users Ids according to the attack submissions of the user, user id is used in each and every submission Na and after that select 6 groups of data which Na= 5, 10, 15, 20, 25, and 30 respectively. There are 300 normal users in the system, in these 6 groups of data, the malicious users have taken up 1.6%, 3.2%, 4.8%,6.2%, 7.7% and 9% of the total user number. They are selected to represent attacks with very small, small, medium, large and very large number of malicious users. Attacks with a larger number of malicious users usually have stronger attack power and may cause larger attack impact.

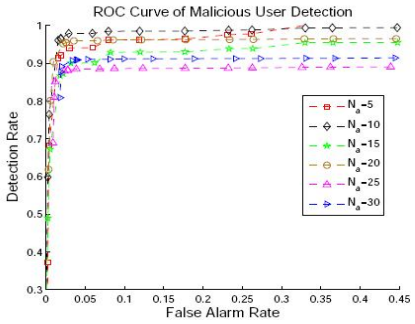

Figure 1 shows the ROC curves for malicious user detection for different *Na* values. The proposed scheme has demonstrated a consistent good performance in detecting malicious users. When the false alarm rate is around 5%, it yields high detection rate (i.e.> 88%) for all attacks with different number of malicious users. As a summary, the proposed scheme has achieved a very good Performance in terms of accurately identifying malicious users. In the future work, we will continue to evaluate the performance of the proposed scheme in terms of recovering reputation score of the target items. These based on the perfect identification of malicious users, the proposed scheme has demonstrated a great potential to reduce the reputation distortion caused by malicious users' dishonest ratings, and keep the online reputation system a secure

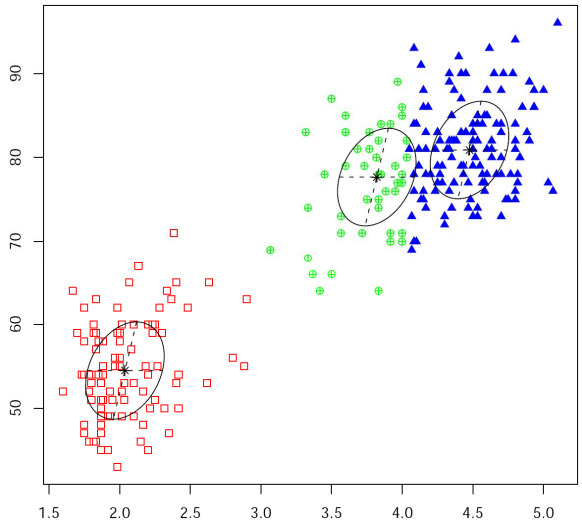

Fig.2 .separating suspicious ratings by using clusters

Fig,2 shows the grouping of reputations which was provided by malicious users, here we are separating the suspicious comments of a particular user with the help of cluster based approach .In figure 2 we are separating the each and every users behaviours by identifying their user id and later we are calculating the behaviour of the particular user . With this cluster based approach we can easily observe each and every users actions,

IV. Conclusions

The proposed detector is used to detect whether changes occur in the ratings of an item and also Estimate the time when attacks are suspected that is which rating is suspicious; with the help of these suspicious ratings we can easily identify the malicious users. By using this cluster based scheme we can group or separate unwanted users reputations.

References

Yafei Yang, Qinyuan Feng, Yan Sun, and Yafei Dai, "Reputation trap: An powerful attack on reputation system of file sharing p2p environment," in *Proceedings of the 4th International Conference on Security and Privacyin Communication Networks*, Sep 2008.

M. Abadi, M. Burrows, B. Lampson, and G. Plotkin, "A calculus for access control in distributed systems," *ACM Transactions on ProgrammingLanguages and Systems*, vol. 15, no. 4, pp. 706–734, 1993.

H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending
against sybil attacks via social networks," in *Proceedings of the 2006 conference on Applications, technologies,architectures, and protocols for computer communications*, pp. 267-278, 2006.

A. J_sang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th Bled Electronic Commerce Conference*, 2002. [5] J. Weng, C. Miao, and A. Goh, "An entropy-based approach to protecting rating systems from

unfair testimonies," *IEICE TRANSACTIONS on Information and Systems*, vol. E89–D, no. 9, pp. 2502–2511, Sep 2006.

A. Whitby, A. J_sang, and J. Indulska, "Filtering out unfair ratings in bayesian reputation systems," in *Proceedings of the 7th Int. Workshop on Trust in Agent Societies*, 2004.

J. Zhang and R. Cohen, "A personalized approach to address unfair ratings in multiagent reputation systems," in *Proc. of the Fifth Int. Joint Conf. on Autonomous Agents and Multiagent Systems (AAMAS) Workshop on Trust in Agent Societies*, 2006, pp. 89–98.

P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu, "Information filtering via
iterative refinement," in *Europhysics Letters*, pp. 1006-1012, 2006.

Y. Liu and Y. Sun, "Anomaly detection in feedback-based reputation systems
through temporal and correlation analysis," in *Proc. of 2nd IEEE Int. Conference on Social Computing*, Aug 2010.

G. Shafter, *A Mathematical Theory of Evidence*, Princeton University Press, 1976.

AUTHOR PROFILE

A.Deepthi Priyanka, pursuing M.Tech (CSE) from Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.

Punugoti Srikanth, Assistant Professor (CSE Department), Holy Mary Institute Of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.

Janapati Venkata Krishna, Associate Professor & H O D (CSE Department), Holy Mary Institute Of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.