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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Combination of Trust Evaluation and User Correlation in Online Reputation System For Detection of Malicious user

Vrushali G Chabilwad, Prof.A.D.Gujar

PG Student, Dept. of Computer Engineering. TSSM's BSCOER, Narhe, Pune, Savitribai Phule Pune University, Maharashtra, India.

Associate Professor, Dept. of Computer Engineering. TSSM's BSCOER, Narhe, Pune, Savitribai Phule Pune University, Maharashtra, India

ABSTRACT: Increase in the development of reputation systems in various online social networks, manipulations against such systems are evolving quickly. Internet has many sources to work together with unknown persons. There are numerous types of risks concerned in it. Real user attack data collected from a cyber competition is used to construct the testing data set. Here we, suggested system is depending on maintaining overall scores by removing harmful scores as well as determining harmful user. Ranking recovery and harmful user recognition is done by utilizing change detection algorithm and believe in model depending on Dempster Shafer theory. Here important thing is to identify harmful rating, it under attack as well as the harmful user recognition

KEYWORDS: Reputation System, Information Security, User correlation, Trust Evaluation.

I. INTRODUCTION

A reputation system is a system which determines and changes reputation ratings for particular things (here, item) within specified domain, based on viewpoint of the client or user that others hold about item. The views of clients or user are generally approved as ratings to a frequent position where all viewpoint and ratings of the client and user are saved and prepared. A reputation system center which utilizes a criteria to estimate runtime overall reputation ratings based on ratings obtained. Reputation system is where we can believe in as opinions by other individuals to the item that they utilization. Here are the objectives regarding aspects such as visibility factor, availability factor, and privacy aspect of individuals that provide ratings to the item. The administration of popularity the exposing of personal and delicate details and other relevant activities is significant element to how individuals work together in n/w as they expose the delicate data, develop believe in with other user, and gather needed information to fix the issues and get details of the item. People build utilization of reputation ratings viz. entire ratings for making decisions when customer believes of buying any item. A item having a very high scores will usually generate more fascination in business than a item with a lower ranking. Hence interest relies on the reputation score or the ratings to the item.

As combined reviews in a group assign a item's reputation score based on ratings, a reputation system signify a form of communicative acceptance. A low ranking symbolizes a sanctioning collaboratively of an item that the group believes having cheaper quality to that item. In turn, a greater reputation scores declares means excellent top quality to that specific item. Reputation ranking is dependent upon inbound ranking, hence Reputation ranking modify centred on the ranking provided by user. There can be damage of greater values if user starts supplying low values and vice-versa. Reputation techniques are relevant to recommender techniques and collaborative filtration, but with the distinction that reputation techniques generate scores centred on precise scores from the group, whereas recommender techniques utilization some external set of organizations and events (such as the purchase of books, movies, or music) to produce marketing suggestions to users. The part of reputation techniques is to accomplish trust, and often features by making the reputation more visible. [3][4]

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

The need of reputation system is applied in huge social networks as a certain client or the user can have entertaining interaction to other customers or customers who are lack of experience. This conversation can help to build decisions. In this paper, suggested system deals with a reputation defense scheme, using Believe in Assessment and User Connection for reviews from customer's reputation system. Proposed plan includes two blocks: a modify detector and a trust prevent based on the Dempster Shafer theory. Here, the scores are considered on basis of time sequence and modify sensor examines dubious time durations where changes take place. The trust prevent will determine trust values and to identify behavior pattern which will in turn figure out whether user scores are reliable or untrustworthy.

Section II discusses related work, Section III describes Proposed System, and Section IV describes, Experiments and Result followed by the conclusion in Section V.

II. RELATED WORK

With the significant development of available information, particularly on the World Wide Web, evaluation-based filtration has become an essential process. Several frameworks are used planning to type through massive amounts of information and select what is liable to be more essential.

Basic Framework

P. Laureti, L. Moret, Y.-C. Zhang and Y.-K. Yu [3] have analyzed a new scoring structure that brings together the tests of N agents over M objects by usage of reputation and weighted. An important aspect of information filtering regards scoring systems in the World Wide Web. They collect evaluations and aggregate them into published scores that are meaningful to the final user. This embraces many different instances, ranging from commercial websites, where buyers evaluate sellers to new generation search engines (Google, Yahoo, etc.), and opinion websites, where people evaluate objects Opinions, Tail rank, etc.) Since the evaluators carry different expertise, it is important to estimate how accurate a given vote may be and to weight it accordingly. This can be done through the use of raters' reputations. Reputation summaries one's past behavior and has always been used to bear the risk of interacting with strangers. The Internet, while enhancing such a risk, brings in the possibility to find its antidotes.

Improvements in basic framework

As the worth of reputation frameworks is well known, the enticement to manipulate such frameworks is rapidly creating. In the research by Y. Liu and Y. Sun [4], In this paper, we model the feedback-based reputation systems as the system in which users provide ratings to objects. This model can describe many practical systems. For example, buyers provide ratings to products on Amazon.com, and members rate local shops on Epinions.com. The objects in above systems are products and shops, respectively. The ratings in our system take integer values from 1 to 5. In reality, one user may provide several ratings for the same object, and we only count one. In addition, many users provide ratings and reviews at the same time. Note that the reviews may be untruthful. In this work, we only consider ratings. The analysis on the reviews and the TAUCA scheme complement each other. The simulator results and case research have showed that the RepTrap attack can essentially reduce the sources needed to strike popular items. With the similar sources, the good results possibility of attacks was extremely enhanced. The more extensive impact of this strike and a few versions of RepTrap were furthermore analyzed.

H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman [8] presented Sybil Guard; Defending against Sybil attacks without a trusted central authority is much harder. Many decentralized systems today try to combat Sybil attacks by binding an identity to an IP address. However, malicious users can readily harvest (steal) IP addresses. Note that these IP addresses may have little similarity to each other, thereby thwarting attempts to filter based on simple characterizations such as common IP prefix. Spammers, for example, are known to harvest a wide variety of IP addresses to hide the source of their messages, by advertising BGP routes for unused blocks of IP addresses [2]. Beyond just IP harvesting, a malicious user can co-opt a large number of end-user machines, creating a bonnet of thousands of compromised machines spread throughout the Internet.

Bayesian A. Jsang and W. Quattrociocchi [5] In the case of centralized reputation systems, ratings are collected centrally and the computed reputation scores are its private reputation ratings it can also use what we refer to as the "public reputation" of the advisor agent. Experimental outcomes display the stability of the customized technique

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

regarding contouring provider's reliability targeted around the rates of unfair scores they provided. Stability of guide agents will be reduced all the more/less if guide agents give more/less unfair scores. Their technique can effectively model the reliability guide basically when client agents do not have much participation with provider agents. Besides, their technique is still practical when the most part of guide agents give variety of bogus ratings, by acclimating to rely all the more intensely on private standing of guide agents Y. Liu and Y. L. Sun [9] a complete anomaly detection plan, TAUCA, was composed and assessed for securing feedback based online reputation frameworks. To examine the time-domain data, an amended CUSUM detector was created to discover suspicious intervals. To evacuate legit ratings in the suspicious interims, similarity computation and clustering systems were utilized to recognize the colluded malicious clients. Genuine client attack information was utilized as a part of performance assessment. Contrasted with IR and Beta model, TAUCA accomplished comparative recuperated reputation offset esteem, however much higher detection rate in malicious client detection.

III. PROPOSED ALGORITHM

A. *Description of the Proposed Algorithm:*

In Momentary and Trust Evaluation, the suggested system to identify changes from a various point of view evaluate time domain information. First the ratings are organized sequentially in climbing down order. The series gives concept of ranking pattern given item. Several items have natural and stable quality, which would give concept of submission of ranking given by the users.

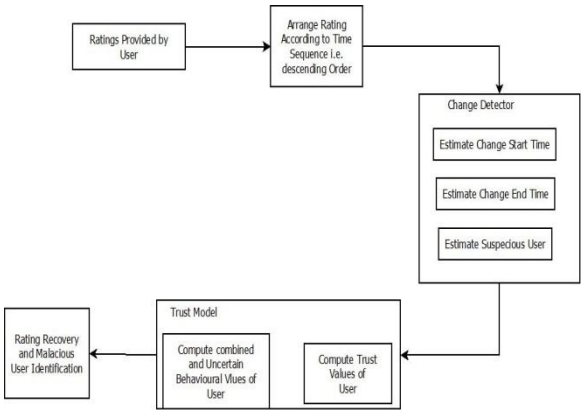

Fig1. An overview of Reputation System with defense scheme

Assume there is unexpected or fast modify in ranking then we can say that there is an abnormality. Therefore, modify detector is suggested as abnormality detector, in which ranking series is the input and shows modify in the series of ranking. The change detector suggested in this paper will not only identify unexpected fast changes and also little changes eventually. Hence, if harmful user places bogus ratings with little period the popularity ratings of such type of changes will still be recognized by suggested modify detector model. Time durations in which frequent changes continue to persist are called as "change intervals".

Algorithm

Algorithm 1 Change Detection:

1: User gives the input in form of ratings at a specific time period.
2: The ratings are arranged in descending order considering the time that the ratings are provided.
3: Calculate CUSUM function (Equation 1) on the rating provided and find the maximum of all.
4: If the maximum function is greater than the threshold the particular item is considered under attack.
5: Now for each CUSUM function computed for all rating, if the value is greater than the threshold then Compute Change in starting time (Equation 2): as well as set alarm to 1 else if less than the given threshold then simulate change in ending time (Equation 3) as well as set alarm to 0.
6: Output: Change in starting time, change in ending time and the suspicious user.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

There are many change detector system developed based on the system utilized [13], [14]. However, regular ranking do not follow a specific design and the intruders may place bogus scores with little modify, we select a special change detector which is not delicate to PD (Probability Distribution) and even identify little modify in changes. Hence, CUSUM detector is chosen [14].
But the outcomes viz. dubious acquired from change detector still may contain regular users. So, to gain precision a believe in model is built where believe in values of each user is determined and harmful user is determined.

Algorithm 2 Trust model:

1: Consider user rating to a particular item and to other items.
2: Calculate behavior value and determine the values used for calculating the combined behavior of the user. If the behavior value is 0 then its r and if behavior value is1then is s as r and s is used in calculating combined user behavior.
3: Combined behavior value (Equation 4) of a particular user using the r and s values.
4: Calculate behavior uncertainty (Equation 5).
5: Calculate trust values (Equation 6) for the user giving rating to many items and trust values for a user to single item (Equation 7).
6: Calculate total trust values of users.
7: If the total trust value (Equation 8) of a user is less than the threshold the user with trust values are said to be malicious.

As the outcome obtained from change detector still can contain usual users. Therefore, to improve or gain accuracy a trust model is built where trust values of every user are designed and malicious user are identified. Important concepts used in trust model:

- Behavior Value: When user gives scores to items or item and is recognized by change detector model, then behavior value is set to 0 or else 1. These values are depending on how frequently ranking given by user to one item.

- Combined Behavior Value: When user gives scores too many items or items and is recognized by change detector, then behavior value is 0 or else 1. This is relied upon how frequently ranking given by user to many item. This can be measured as:

$$Beh_{uj}^{com}(i) = r/ (r+s+2)$$

- Behavior Uncertainty: In the same way, we figure out a user behavior un-certainty with help of Dempster Shafer concept. This can be measured as:

$$Beh_{uj}^{uncer}(i) = r/ (r+s+2)$$

Finally, depending upon the trust values of the user the username is recognized some significant formulas for determining the fake ratings and the malicious user identification are:

1) CUSUM detector function:

$g_k = \max (g_{(k-1)} \ln \frac{p_{\Theta 1 (y(k))}}{p_{\Theta 0 (y(k))}}, 0)$

2) Change in start time:

$t_s = \arg\max (t1 \leq c \leq t) \sum_{i=t1}^{c-1} \ln \frac{p_{\Theta 1 (y(k))}}{p_{\Theta 0 (y(k))}}$

3) Change in end time:

$t_e = \arg\max (t1 \leq c \leq tb) \sum_{i=d+1}^{(tb)} \ln \frac{p_{\Theta 1 (y(k))}}{p_{\Theta 0 (y(k))}}$

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

4) Combined behavior value:

$Beh_{uj}^{com}(i) = \frac{r}{(r+s+2)}$

5) Behavior Uncertainty:

$Beh_{uj}^{com}(i) = \frac{2}{(r+s+2)}$

6) Trust value based on many items:

$T_{uj}^{com}(i) = Beh_{uj}^{com}(i) * (1\text{-}Beh_{uj}^{uncer}(i))$

7) Trust values based on one item:

$T_{uj}^{com}(i) = Beh_{uj}^{com}(i) * Beh_{uj}^{uncer}(i)$

8) Total trust (T):

$T = T_{uj}^{com}(i) + T_{uj}^{com}(i)$

IV. RESULTS

The following table show False Alarm rate and Detection rate of the proposed system, These rate are totally depend on total number of users and total number of malicious user.

Table 1: False Alarm Rate and Detection Table

Total no. of User	Total no. of Malicious user	False Alarm rate	Detection Rate
174	58	0.333	0.4088
170	66	0.38823	0.4654
161	61	0.4563	0.3788

Following graph represent the false Alarm rate and Detection Rate, both are changes according to the Total number of user and Total number of Malicious user.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

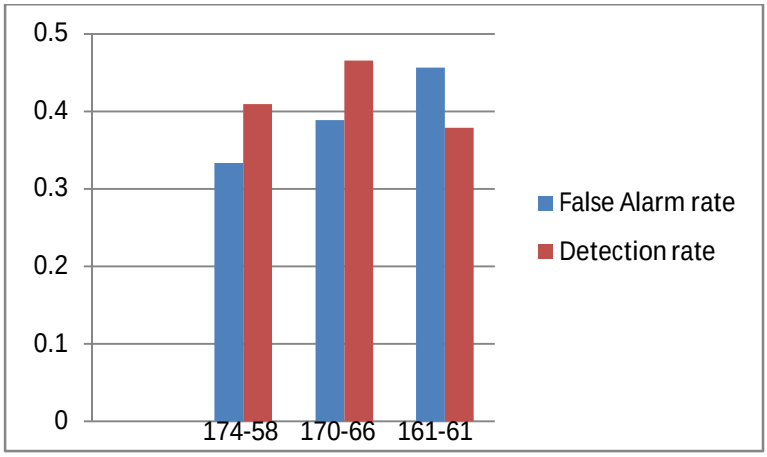

Fig. 2.False alarm rate and Detection rate depend on no. of user and malicious user.

In above graph X-axis represent total no.of user and total no.of malicious user and Y-axis represent rate value and graph represent false alarm rate and detection rate depend on no.of user and malicious user.

V. CONCLUSION AND FUTURE WORK

In this paper, a protection schema is efficiently applied which recognizes malicious user as well as restoration of the regular user scores. The change detector system and trust model performs a crucial role or they are center of fascination in the suggested system.

In future work, the retrieved regular ratings should be secured while interaction between web server and the suggested defense scheme so as to avoid from user in the middle attack.

REFERENCES

1. P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," Common. ACM, vol. 43, no. 12, pp. 4548, 2000.
2. C. Dellarocas, "The digitization of word-of-mouth: Promise and challenges of online reputation systems," Management Science, vol. 49, no. 10, pp. 14071424, October 2003.
3. P. Laureti, L. Moret, Y.-C. Zhang and Y.-K. Yu, "Information filtering via iterative refinement," Europhys. Lett. vol. 75, no. 6, pp. 10061012, 2006.
4. Y. Liu and Y. Sun, "Anomaly detection in feedback-based reputation systems through temporal and correlation analysis," in Proc. 2nd IEEE Int. Conf. Social Computing, Aug. 2010, pp. 6572.
5. A. Jsang and W. Quattrociocchi, "Advanced features in Bayesian reputation systems," Trust Bus, pp. 105114, 2009.
6. J. Zhang and R. Cohen, "A personalized approach to address unfair ratings inmultiagent reputation systems," in Proc. Fifth Int. Joint Conf. Autonomous Agents and Multi-agent Systems (AAMAS) Workshop on Trust in Agent Societies, 2006, pp. 8998
7. Y. Yang, Q. Feng, Y. Sun, and Y. Dai, "Reputation trap: A powerful attack on reputation system of file sharing p2p environment," in Proc. 4th Int. Conf. Security and Privacy in Communication Networks, Istanbul, Turkey, Sep. 2008.
8. H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybil guard:Defending against Sybil attacks via social networks," in Proc. 2006 Conf. Applications, Technologies, Architectures, and Protocols for Computer Communications, 2006, pp. 267278.
9. Y. Liu and Y. L. Sun, "Detecting cheating behaviors in cyber competitions by constructing competition social network, poster track," in IEEE Intl. Workshop Information Forensics and Security (WIFS11), Brazil, Nov. 29Dec. 2 2011.
10. M. Gomez, J. Sabater-Mir, J. Carbo, and G. Muller, "Improving the arttest bed, thoughts and reflections," in Workshop on Competitive agents in Agent Reputation and Trust Test bed, Salamanca, 2008, pp. 115
11. J. Werther, M. Zhivich, T. Leek, and N. Zeldovich, "Experiences in cyber security education: The mitlincoln laboratory capture-the check alarm exercise," in Cyber Security Experimentation and Test, 8 August 2011.
12. CANT, http://www.ele.uri.edu/nest/cant.html.
13. W. A. She what, Economic Control of Quality of Manufactured Product. Princeton, NJ, USA: Van Nostrand, 1931.
14. S. Page, "Continuous inspection schemes," Biometrika, vol. 41, no. 1/2, pp. 100115, Jun. 1954.
15. Yuhong Liu, Yan (Lindsay) Sun, Siyuan Liu, and Alex C. Kot, "Securing Online Reputation Systems through Trust Modeling and Temporal Analysis", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 6, June 2013

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

BIOGRAPHY

Vrushali G. Chabilwad has received Bachelor of Engineering in Information Technology from MGM's,Jawaharlal Nehru Engineering College ,Aurangabad. India in 2012. And pursuing Master of Engineering from TSSM's Bhivarabai Sawant College of Engineering and Research,,Narhe,Pune, India. Her research interest is networking, security and data mining.

Prof A.D.Gujar is full time Associate Professor at TSSM's BSCOER,Narhe Pune,India .He has Completed M.Tech in Information Technology and his research interest is networking and network security.