Securing Online Reputation System Through Trust Evaluation And User Correlation

[1]D.Gnana Binu, [2]R.Ravi, [3]Dr. Beulah Shekhar
[1]PG Scholar, Department of Network Engineering, Francis Xavier Engineering College, Tirunelveli.
[2]Professor& Head, Department of Computer Science and Engineering, Francis Xavier Engineering College,Tirunelveli, Tamil Nadu State, India.
[3]Associate Professor, Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu State, India.

Abstract— **Online Reputation Systems are playing increasingly important roles in influencing people's online purchasing/downloading decisions. In this paper we propose a scheme user correlation algorithm. The existing mechanisms Time Domain Anomaly detection and Trust model based on dempster safer theory not provide better efficiency. First, limit the maximum number of ratings each user could provide with in the certain time duration. Second investigating users rating behaviors by building user trust, such as a personalized trust model, which evaluates a user's judging power as the inverse of this user's rating variance. In the proposed system, jointly consider trust evaluation and user correlation. Correlation is calculated based on already defined malicious users. Based on the user correlated relationship values eliminate the time consuming and low efficiency.**

Index Terms—: Network Security, Time Variation, Trust Evaluation, User Correlation, Rating Sequence

1 INTRODUCTION

Now a day, the website created by online communication. For ordinary users trust a stranger useful and the quality is difficult to assess. This is dangerous as online communication. The problem is how to find online stock good quality product. Using this online reputation system. The main objective is to share opinions and experiences unique to the mouth network are to create a large scale virtual word. By providing different product evaluation. And evidence collected, compiled and analyzed public opinion, those people that are disseminated to users based on their opinions and experiences. Popularity score results are disseminated. These systems are referred to as concept -based reputation systems. Most people find the product evaluation before purchasing a particular product. Many online reputation systems is evolving rapidly. Many programs automatically insert the generated ideas. Some reputation management companies that provide services to assess their customers provide the real user ID.

More items on the offensive against the scores of famous reputation systems, online reputation systems can increase the confidence of users in an accident, caused economic loss. It is therefore urgent to protect the online reputation system. Again, in terms of reputation feedback systems security program has a reputation of Tata, Tata joint temporary and wrinkles Foundation study [1]. Dempster secure domain at a time anomaly detector and a trust model based on the principle: it has two modules. At the time of order and disorder, there will be a time domain is introduced to detect suspicious anomaly detection time interval to a particular item rating [4] In. Faith estimate of the anomaly detection is performed based on the results [1]. Each item is a model user behavior and user feedback evaluation to assess the uncertainty of the user's behavior or not. This reliable method can provide better performance. We have confidence in the assessment and analysis of user interaction [2] propose to connect the system is introduced. Faith estimate is calculated using the means of communication with the malicious user to identify the malicious user. This method can improve the performance and efficiency.

Manuscript received Feb, 2013.

D.Gnana Binu*, Network Engineering, Anna University/ Francis Xavier Engineering College Tirunelveli ,Tamil Nadu, India, 9487372403*

R.Ravi*,,Computer Science&Engineering, Anna University/ Francis Xavier Engineering College. Tirunelveli, Tamil Nadu, India, 9487372403*

Dr. Beulah Shekhar*, [3]Associate Professor, Department of Criminoloand Criminal Justice, Manonmaniam Sundaranar University,, Tirunelveli,Tamil Nadu State, India.*

II. RELATED WORK

There are so many existing models available for protecting the Reputation system from different techniques. First, The many ratings provided by each user within the certain time duration [1]. Second, same user ID provide the rating to the same product for multiple times. So there are multiple fake identities available this considered Sybil attacks [5].Third, investigating users' rating behaviours by assigning the trust value to each user if the user having higher trust value considered good user, user having lower trust value considered malicious user to identify this by using Trust Evaluation [2]. Fourth, investigating rating distributions by using correlation method used [1].After this the malicious user identified & the accurate score of the particular product identified.

III. SYSTEM MODEL

In this paper, People purchase their product through online. But people we don't know which product is good and which one is bad, for that using online reputation system. Reputation system means assign rating to each products. Rating can be provided through 1 to5. Buyers provide rating to product on OLX.com, AMAZAN.com & Watch a video on you tube. Sometimes the attacker provides higher rating value for the low quality product. For that buyer purchase the low quality product. The attackers identified by using the method Trust Evaluation and User Correlation method.

A. Trust Evaluation & User Correlation

1. General Description

The proposed method contains two techniques: (i) Trust Evaluation and (ii) User correlation. In this, we propose to detect the attacker from different angles change detector used to detect the attacker with in a particular time interval. But in this method sometimes normal users may provide rating value too high or too low due to their unusual experience. So we considered normal user also attacker. Using trust Evaluation method that identify the attacker by calculating the trust value if the user having higher trust value above the threshold value consider good user. The user having lower trust value below the threshold value, then consider it as a malicious user. After identifying the malicious user the user correlation can be calculated by using the correlation algorithm. Finally, the malicious user identified and the ratings to the detected product are removed. The remaining ratings used to calculate the product reputation. Fig.1 describes the architecture of Trust Evaluation & User Correlation method. The design details will be described in the rest of the section.

2. Changing in Rating Sequence

In this the rating sequence can be provided by the user who is purchase their product through online .Here the malicious users can be identified by the user providing the rating with in a particular time interval. For example if one user providing the rating at time 11.00 and the same user providing the rating value at time 11.01, 11.02 etc. Then we consider that user is a malicious user. In particular time interval normal users also provide rating value. So we cannot consider that user is a malicious user. So go to the trust analysis method for identifying that user is a malicious user or not.

3. Trust Evaluation

In this user provide ratings during the particular time interval demonstrate as malicious user. In the particular time interval normal users also provide the rating value. Malicious user identified by trust evaluation method. Here belief theory used that is assigning a trust value to each user. The trust value depends on their good and bad behaviour. Having one threshold value, the trust value below the threshold value consider malicious user. The trust value above the threshold value considered that the user is a good user.

Number of good ratings = without malicious users

Number of Bad ratings = with malicious users

4. Calculation of Correlation

After identifying the malicious user the user correlation can be calculated. The correlation calculated by the formula

$$\textbf{Suspicious score} = \frac{\textbf{(Probability of good ratings + Probability of bad ratings)}}{\textbf{(Probability of total no.of ratings)}}$$

The suspicious score calculated for the particular product based on the method. After identifying the score we demonstrate that product is a good product or bad product.

5. Identification of Malicious User

Based on the time interval and rating provided with the same mail id identifying the malicious user. If there is a variation in time must be large means we consider malicious user1. The variation must be little small means we consider malicious user2.The variation must be very small considered malicious user3. The user providing the rating with the same mail id and the time variation based on this we considered malicious user.

6. Product Reputation Score

After identifying the malicious user for the particular product the original rating for the product calculated. After we identifying that product is good or not.

Here first we are providing the product ratings after that are arranged in ascending order based on the time the ratings are arranged. After identifying if there is any attack available attack can be detected by the time interval that is rating provided within a particular time interval then there is an attacker available. No attack means that the product is good. If attack means go to the next process trust evaluation. Here assigning the trust value to each user. If the user trust value high means that the user is good and no attack available. The trust value high means there may be an attack available. In the step correlation calculate the suspicious score for the particular product and evaluate the product. Identify the malicious user based on the trust value provided. There are three types of malicious user available. There is a large variation in time interval considered malicious user1. If the variation in time interval a little small means consider malicious user2. There is a variation in time interval very small considered malicious user3. The users who are providing the correct rating value consider the good user and the product is good. The correct score of the product identified. After we demonstrate that the product qualification.

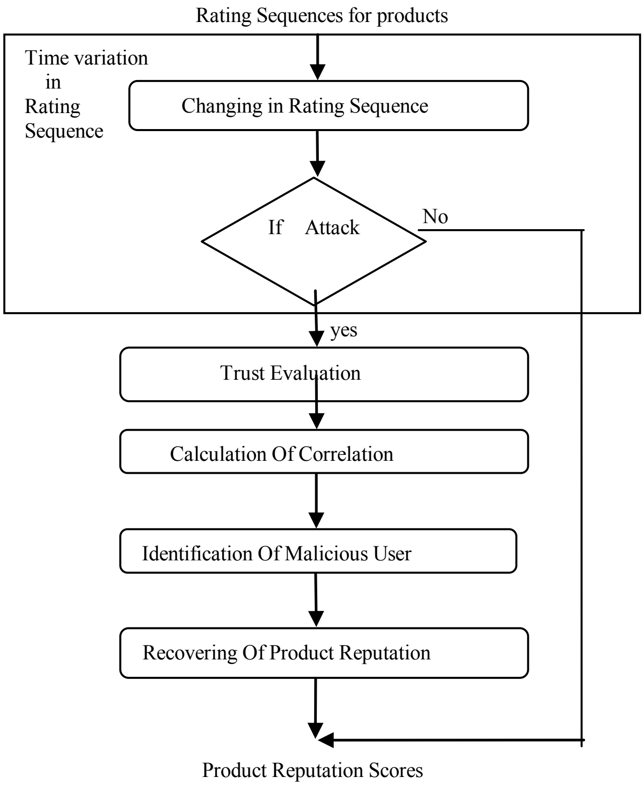
Rating Sequences for products
Time variation in Rating Sequence
Changing in Rating Sequence
If Attack
No
yes
Trust Evaluation
Calculation Of Correlation
Identification Of Malicious User
Recovering Of Product Reputation
Product Reputation Scores

Fig1.System Architecture

IV. EVALUATION

After finding the suspicious score we evaluate the score that based on the total ratings, good ratings and bad rating that evaluate the time complexity for the particular product.

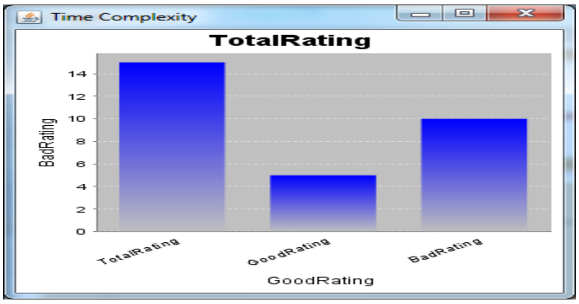

Fig. 2 Suspicious Score Evaluation

V. DISCUSSION

In this paper, we discuss some limitations of our system. Currently, trust model and time domain anomaly detection method provide less efficiency and used only for detecting small amount of malicious users. When combining user correlation and trust evaluation method provide more efficiency and detect a large number of malicious users.

VI. CONCLUSION

Previous methods like trust model based on dempster safer theory and time domain anomaly detections are providing less efficiency and detect small amount of malicious users. When the number of malicious user is very large, this method is not good. In the proposed, is to jointly consider trust evaluation and user correlation method. Through this, we can eliminate the time consuming, low efficiency and when the number of malicious user is large compared with the previous one this method is a good one. This method is to çalculate the suspicious score for the particular product. Finally, product evaluation gives the time complexity for the particular product.

ACKNOWLEDGMENT

First of all we thank the almighty for giving us the knowledge and courage to complete the research work successfully. We express our gratitude to our respected Professor and Head of CSE R.Ravi., for following us to do research work effectively.

REFERENCES

1. 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. 65–72.
2. Whitby, A. Jøsang, and J. Indulska, “Filtering out unfair ratings in Bayesian reputation systems,” Icfain J. Manage. Res., vol. 4, no. 2, pp.48–64, Feb.
3. P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu, “Information filtering via iterative refinement,” Europhys. Lett., vol. 75, no. 6, pp.1006–1012, 2006.
4. Yuhong Liu, Yan (Lindsay) Sun, Siyuan Liu, and Alex C. Kot, Securing Online Reputation Systems Through Trust Modeling and Temporal AnalysisR. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, “High-speed digital-to-RF converter,” U.S. Patent 5 668 842, Sept. 16, 1997.
5. H.Yu,M. Kaminsky, P. B. Gibbons, and A. Flaxman, “Sybilguard: Defending against sybil attacks via social networks,” in Proc. 2006 Conf.Applications,Technologies, Architectures, and Protocols for Computer Communications, 2006, pp. 267–278
6. 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.
7. M. Abadi, M. Burrows, B. Lampson, and G. Plotkin, “A calculus for access control in distributed systems,” ACM Trans. Program. Lang.Syst., vol. 15, no. 4, pp. 706–734, 1993.
8. H. Yu,M. Kaminsky, P. B. Gibbons, and A. Flaxman, “Sybilguard: Defending against sybil attacks via social networks,” in Proc. 2006 Conf.Applications, Technologies, Architectures, and Protocols for Computer Communications, 2006, pp. 267–278.
9. J. Weng, C. Miao, and A. Goh, “An entropy-based approach to protecting rating systems from unfair testimonies,” IEICE Trans. Inf. Syst.,Vol. E89-D, no. 9, pp. 2502–2511, Sep. 2006.
10. Jøsang andW. Quattrociocchi, “Advanced features in bayesian reputation systems,” TrustBus, pp. 105–114, 2009.

D.Gnana Binu is doing her M.E in Francis Xavier Engineering College at Tirunelveli. She received her B.E degree in Computer Science Enigineering from DMI College Of Engineering, Chennai in 2012. She is an active member of the Computer Society of India(CSI). Her area of interest s are Networking, Network Security, Mobile Computing and Data Structure.

Dr. R. Ravi is an Editor in International Journal of Security and its Applications (South Korea). He is presently working as a Professor & Head and Research Centre Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He completed his B.E in Computer Science and Engineering from Thiagarajar College of engineering, Madurai in the year 1994 and M.E in Computer Science and Engineering from Jadavpur Government research University, Kolkatta. He has completed his Ph.D in Networks from Anna University Chennai. He has 18 years of experience in teaching as Professor and Head of department in various colleges. He published 12 International Journals, 1 National Journal. He is also a full time recognized guide for various Universities. Currently he is guiding 18 research scholars. His areas of interest are Virtual Private networks, Networks, Natural Language Processing and Cyber security.

Dr. Beulah Shekhar is a Coordinator for Victimology & Victim Assistance, in the Department of Criminology and Criminal Justice Sciences; she is presently working as a Associate Professor in the Department of Criminology and Criminal Justice Sciences. And her areas of interest are Crimes against Women Empowerment, Human Rights, and Police Training.