International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Survey for Detecting Malicious user using Trust Evaluation and User Correlation for Protecting Online Reputation Systems

Vrushali G. Chabilwad[1], A. D. Gujar[2]

[1]TSSM's Bhivarabai Sawant College of Engineering and Research, Pune University, Pune, Maharashtra, India

[2]Professor, TSSM's Bhivarabai Sawant College of Engineering and Research, Pune University, Pune, Maharashtra, India

Abstract: ***Over last few years numbers of people are using Internet for Social Networking, Businesses and entertainment. Because users are unknown of third party, it is quiet difficult for users to evaluate honesty and quality of third party. So it is becoming a risky task to perform an online transaction. Large scale research is going on reputation systems. With the fast improvement of reputation systems in different online social networks, exploitations against such frameworks are advancing rapidly. To tackle this problem, a system can be implemented, which secures reputation systems from another point: the combination of time domain anomaly detection and Dempster–Shafer hypothesis based trust calculation. Genuine client assault information gathered from a digital cyber competition is utilized to build the testing data set. Evaluated with two representative reputation plans and existing system, Temporal And Trust Analysis attains an essentially improved performance regarding distinguishing items under attack, discovering malicious clients who embed fraudulent ratings, and improving reputation scores.***

Keywords: Reputation systems, Anonymity, Information security, Information filtering

1. Introduction

As numbers of individuals utilize the World Wide Web for amusement, Social Networking and Businesses, the World Wide Web has opened number of doors for online communications. But, because of the anonymity of the World Wide Web, it is exceptionally troublesome for ordinary users to assess a more stranger's dependability and quality, which makes online collaborations insecure. There are number of questions which challenge the efficiency of products or content that websites have made. Much of the time, the answers can barely be anticipated before the communications are submitted. The issue is the manner by which the online members secure themselves by reviewing the quality of strangers previously. To address this issue, online reputation frameworks have been developed.

The objective is to build substantial word-of-mouth systems where people share feelings and opinions, as far as reviews and ratings, on different things, consisting items, services, digital contents and considerably other individuals. These feelings and opinions, which are called users' feedback, are gathered as proof, and are examined, aggregated, and distributed to general clients. The distributed results are called reputation score. Such frameworks are additionally called as feedback-based reputation frameworks. Online reputation frameworks are progressively affecting individuals' online buying/downloading choices. For instance, items or administrations with a 5-star rating could get 20% more than items or services with a 4-star rating could [1].

More individuals refer to check rating framework before selecting restaurants or hotels; to Amazon item evaluations before buying items online; to YouTube video ratings before review a video; and so on. Besides, a study demonstrates that around 26% of adult Internet clients in the U.S. have evaluated no less than one item through online reputation frameworks [2].

Meanwhile, determined by the tremendous benefits of online markets [3], various exploitations against online reputation frameworks are advancing quickly. Numerous complex projects are produced to automatically insert feedback. Moreover, few reputation management companies even control expansive associate networks of genuine client IDs to give "rating services" for their clients.

2. Literature Review

With the substantial growth of accessible data, particularly on the World Wide Web, evaluation-based filtering has become an important task. Numerous frameworks are applied planning to sort through giant volumes of data and choose what is liable to be more important. P. Laureti, L. Moret, Y.-C. Zhang and Y.-K. Yu [4] have examined a new scoring framework that combines the assessments of N agents over M objects by utilization of reputation and weighted midpoints. Agents, subsequently, are positioned as per their judging ability and objects as per their quality. The strategy can be developed by means of an iterative algorithm, where the inherent bias of the estimators of the weights can be amended. They indicate, with simulations and logical results, that the strategy is powerful and strong against misuses. The bigger the framework, the better is the filtering accuracy. This technique can be applied in web-related reputation and scoring frameworks.

As the worth of reputation frameworks is well known, the inducement to exploit such frameworks is quickly developing. In the study by Y. Liu and Y. Sun [5], 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.

Reputation frameworks are assuming important parts in securing communication frameworks and distributed computing. Like all other security techniques, reputation frameworks can be under attack. Y. Yang, Q. Feng, Y. Sun, and Y. Dai [6] presented the revelation of novel and influential attack, named RepTrap, against feedback-based reputation frameworks. Through a top to bottom examination, they introduced the situations that this attack may be applied to, the approaches to viably lead this assault, and the outcome of the attack. The performance assessment is focused around real information and practical client models in a prominent P2P file sharing framework. The simulation outcomes and case studies have exhibited that the RepTrap attack can fundamentally decrease the resources needed to attack famous items. With the same assets, the success probability of attacks was incredibly improved. The more expansive effect of this attack and a few variants of RepTrap were likewise examined.

Peer-to-peer and other decentralized, distributed frameworks are known to be especially susceptible against Sybil attacks. In a Sybil attack, a malicious client acquires numerous fake identities and puts on a show to be various, different nodes in the framework. By controlling a huge portion of the nodes in the framework, the malicious client has the capacity of "out vote" the legitimate clients in mutual tasks, for example, Byzantine failure defences. H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman [7] introduced SybilGuard, a new decentralized system for restricting the corruptive impacts of Sybil attacks, by limiting both the number and size of Sybil groups. SybilGuard depends on properties of the clients' basic interpersonal network, to be specific that a) the honest area of the system is quick mixing, and b) malicious clients may make numerous nodes however generally less attack edges. In all their simulation with one million nodes, SybilGuard guaranteed that a) the number and size of Sybil groups are appropriately limited for 99.8% of the legitimate clients, and b) a legit node can acknowledge, and be acknowledged by, 99.8% of all other legit nodes.

Bayesian reputation frameworks are truly adaptable and can moderately effectively be adapted to diverse sorts of applications and situations. A. Jøsang and W. Quattrociocchi [8] presented a succinct review of the rich set of peculiarities that describes Bayesian reputation frameworks. Specifically they show the significance of base rates amid bootstrapping, to deal with rating scarcity and for communicating long haul patterns. They obtained conclusion that: Bayesian reputation frameworks have a strong basis in traditional statistics which make them sound and easy to adjust to different settings. Bayesian reputation is good with opinions of biased logic, accordingly permitting computational trust to be consolidated with reputation frameworks. This paper has demonstrated the extraordinary adaptability of binomial and multinomial Bayesian reputation frameworks.

J. Zhang and R. Cohen [9] surveyed distinctive methodologies for tackling unfair ratings, and their benefits and drawbacks. They list the capacities that a methodology ought to have. Approaches for tackling unfair ratings ought to have the capacity to take into account the preference comparability between customer agents and agents. They ought to have the capacity to handle both unreasonably high and low ratings. They ought to additionally have the capacity to handle the changes of agents' behaviour about whether. They compare those current methodologies focused around the four abilities. They then classify these methodologies regarding two measurements, a "public-private" measurement and a "global-local" measurement. They additionally examine the effect of reputation framework architectures on the determination of methodologies for tackling unfair ratings.

Methodologies utilized as a part of centralized reputation frameworks fit in "public" class and cannot consider client agents' individual experience with advisor agents' recommendation (ratings), though methodologies utilized as a part of distributed reputation frameworks fit in the "private" classification and cannot consider all ratings for supplier agents. This classification of the distinctive methodologies gives a significant point of view on the key difficulties confronted in developing a successful reputation framework that makes utilization of recommendation from different agents, however takes consideration to think the dependability of those ratings.

Depending on the study of these methodologies, they presented a personalized methodology for adequately tackling unfair ratings in improved centralized reputation frameworks. The personalized methodology has every one of the four of the abilities. It additionally has the advantages of both methodologies utilized as a part of centralized reputation frameworks and methodologies utilized as a part of distributed reputation frameworks. It permits a client agent to approximate the private reputation of an advisor agent depended on their ratings for normally rated provider agents. At the point when the client agent is not sure with the private reputation value, it can likewise utilize the public reputation of the guide agent. The public reputation of the guide agent is assessed focused on all ratings for the provider agents appraised by the guide agent.

Experimental results exhibit the viability of the personalized methodology regarding conforming agents' dependability focused around the rates of unfair ratings they gave. Reliability of guide agents will be diminished all the more/less if guide agents give more/less unfair ratings. Their methodology can adequately model the reliability of guide actually when client agents do not have much involvement with provider agents. Besides, their methodology is still viable when the most part of guide agents give expansive quantities of unfair ratings, by acclimating to depend all the more vigorously on private reputations of guide agents.

Y. Liu and Y. L. Sun [10] perceived Cyber Competition as a proficient approach to encourage research and training in

cyber security [11] [12] [13]. They have found that the players in cyber competitions can cheat so as to increase a higher rank or gather more prizes. They utilize information gathered from the CANT competition to examine such cheating practices and present to develop a competition social network to identify cheating practices in cyber competitions.

3. Proposed System

We present a reputation protection plan, for reputation frameworks. It consists of two modules a change detection algorithm and a trust model based on the Dempster–Shafer hypothesis. Particularly, we consider the ratings to a given thing as a time sequence, and a time domain change detector is presented to detect suspicious time intervals where anomaly happens. A trust examination is then directed focused around the anomaly detection results. We get the idea of client behavior uncertainty from the Dempster–Shafer hypothesis to model clients' behavior designs, and assess whether a client's appraising quality to every item is dependable or not.

In addition to recovery of ratings this system is going to consider user correlation and trust evaluation in which will calculate the trust values of all the users depending upon the behavior and identify the malicious user depending upon the low trust values among all the users.

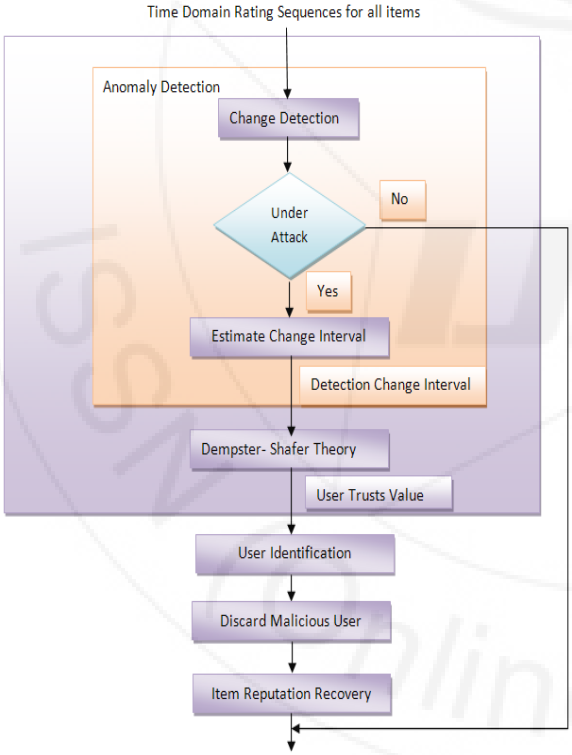

Figure 1: System Architecture

4. Conclusion

In this paper, we surveyed major issues in reputation system and also had look over the improvements required to be obtained in online reputation system. With the fast improvement of reputation systems in different online social networks, exploitations against such frameworks are advancing rapidly. To deal with this issue, we presented a comprehensive anomaly detection scheme. We evaluated it for protecting feedback-based online reputation systems.

References

[1] Press Release: Online Consumer-Generated Reviews Have Significant Impact on Offline Purchase Behavior, Nov. 2007 [Online]. Available:http://www.comscore.com/press/release.asp?press=1928
[2] R. Lee and H. Paul, Use of Online Rating Systems Oct. 20, 2004 [Online]. Available:http://www.pewinternet.org/Reports/2004/Use-of- Online-Rating-Systems.aspx
[3] ComScore, Final Pre-Christmas Push Propels U.S. Online Holiday Season Spending Through December 26 to Record $30.8 Billion Dec. 29, 2010 [Online]. Available:http://ir.comscore.com/releasedetail.cfm?ReleaseID=539354
[4] 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.
[5] 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.
[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] 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.
[8] Jøsang and W. Quattrociocchi, "Advanced features in bayesian reputation systems," TrustBus, pp. 105–114, 2009.
[9] J. Zhang and R. Cohen, "A personalized approach to address unfair ratings inmultiagent reputation systems," in Proc. Fifth Int. Joint Conf. Autonomous Agents and Multiagent Systems (AAMAS) Workshop on Trust in Agent Societies, 2006, pp. 89–98.
[10] 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 (WIFS'11), Brazil, Nov. 29–Dec. 2 2011.
[11] M. Gomez, J. Sabater-Mir, J. Carbo, and G. Muller, "Improving the arttestbed, thoughts and reflections," in Workshop on Competitive agents in Agent Reputation and Trust Testbed, Salamanca, 2008, pp. 1–15.
[12] J. Werther, M. Zhivich, T. Leek, and N. Zeldovich, "Experiences in cyber security education: The mit lincoln laboratory capture-the-flag exercise," in Cyber Security Experimentation And Test, 8 August 2011.
[13] CANT,http://www.ele.uri.edu/nest/cant.html
[14] 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