Providing Security on Online Reputation Sytem Using Rate Auditing Technique (RAT)

D. Dinesh Babu
Assistant Professor
Alpha College of Engineering and Technology
Dept. of Computer Science and Engineering
Pondicherry, India.
dineshbabu89@pec.edu

N. Atchaya
Alpha College of Engineering and Technology
Dept. of Computer Science and Engineering
Pondicherry, India.
akshaya.sivan@gmail.com

B. Chithra
Alpha College of Engineering and Technology
Dept. of Computer Science and Engineering
Pondicherry, India.
chitrabalakrishnan.csc@gmail.com

***Abstract*—In a quick development of world many people using internet. The people using internet for various purposes such as communication between each other, online purchasing, watching videos, playing games etc. Some of the problems or risks can be available in internet such as untrusted ratings. As many number of people refer the ratings and can purchasing through online. This untrusty risk can occur in ratings. To solve this problem only reputation system created in many online social networks. In this paper, we propose the technique of RAT, the abbreviation of Rat Auditing Technique, which protect the reputation system: to monitor each and every rating manipulation and to check the session time of the particular web page. Comparing with our previous scheme, RAT performs better in to detect the attacked items and recovering the reputation scores.**

Keywords*— *Information Security; Social Networking; Information Filtering

I. INTRODUCTION

In this fast developing world, many people using Internet for communicate with one person, business deals and maintaining personal relationships. Internet has built huge possibility for online Services and also internet has created many different opportunities to communicate with unknown person. The communication can be fun, useful or useless. But there are some difficulties for users to unknown untrusting can be able to make online services risky. For example, The advice from a self-proclaimed expect at expert central.com reliable or not is the unknown dot.com site or e-bay seller ship with correct packaging or not. The piece of news is true or not. A product of amazon.com is good? YouTube video is really informative or good? In large number of cases; the answers can be predicted very difficulty. The problem is how the online participants protect themselves by judging the quantity of strangers or unfamiliar items beforehand.

To solve this problem, online reputation systems created. The aim is build a online networks where one person can share his/him own opinions and experiences, by comments and ratings on different items, including products and services. These own opinions and experiences of one individual person are called user's feedback. These information are collected evidence and are analyzed and separated to normal users. The separated results are called reputation to as feedback based reputation systems.

Reputation is an entity it may be a person, an organization give an opinion about that entity. Reputation is important and also used in many places such as business, education, online communities and many other fields. Reputation system is a system which calculates and publishes the reputation scores for the set of objects within a community or domain. It may be of service provides, services, goods or entities. It is based on collections of opinions at other entities hold about objects. Entities in a community use reputation scores for decision making. An object with a high reputation score will normally attract more business than a object with a low reputation score. It is therefore in the interest of objects to have a high reputation score. The collective opinion in a community determines an object's opinions; Reputation systems represent a form of collaborative sanctioning and praising. A low score represents a collaborative sanctioning of an object that the community perceives as having or providing low quality.

The People may using online reputation systems in many applications such as purchasing one items or downloading files or videos etc. For example, according to Co score Inc., 5 star products or service could earn 20% ratings more than 4 star products are services rating [1]. Large number of people uses the rating system before selecting hotels and restaurants, purchasing products online in amazons, viewing a video on a YouTube etc. In US, a recent survey tells 26% adult internet users are rated at least one item through online reputation system [2].

The huge gain in online trade [3], various handling method against online reputation system are develop quickly. Various enlightened programs are created to placing feedback self-activating. Moreover, few reputation management companies control huge networks, they provide "rating services" for their own customers."VideoViralViews.com"[4] can provide 100 real users ratings on one music iTunes. For that music on YouTube, received 30 "I like" and "increase your YouTube". Online securing reputation system is acute.

In this paper, we propose a method RAT for user's opinions and experiences, RAT is the abbreviation of the Rate algorithmic technique. RAT is implementing to monitor each and every rating manipulation. It checks whether the time logged in and logged out matches the stipulated time for viewing any videos or messages and giving the appropriate ratings. It monitors either the video provided is fully or at least partly viewed and then gave the ratings or not. It also checks whether the login in network which is provided rating is either from same location or its location varies each and every time from vast geographical location. Thus by doing this the

attacker is also detected and given counter measures to their attacks.

The performance of other representative schemes [5] [6] and [7] using a cyber competition the real user attack data collected and evaluated. RAT demonstrates the advantages in terms of discard the dishonest ratings under attack and recovering scoring. The rest of paper is followed. Section 2 describes the survey; Section 3 describes the related work. Section 4 describes the existing system; Section 5 introduces the details of RAT, followed by the performance metrics in Section 6 and followed by conclusion in Section 7.

II. SURVEY

The rapid development of using information, especially on the internet, based upon a evaluation filtering become a difficult task. Many systems are aim to sort the information through large volume and select the information which is more relevant. A ranking method [6], analyzed a letter, the reputation information provide the suitable self-consistently. The reputation system value is largely organized, the incentive to handle such system is fast developing. For TAUCA [7], malicious users is identified and recovering reputation scores. In TAUCA, the temporal analysis and user-correlation analysis is combined. The two other representative schemes are tested against the attack data from real user is collected using a cyber competition. The advantages of TAUCA, increases the detection rate and decrease the false alarm rate in detection of malicious users and reduces the bias in reputation scores. In distributed system, the protocols and algorithms are controlled from a logical perspective. The issues in a global distributed system are communication, booting, loading, authentication and authorization. The base of a distributed system cannot reside in single location, under single management. This indicates there is no grantee for secure to provide physically secure communication lines. The account [9], making the request from one side to other side and provide the logical language for control lists and deciding the granted requests.

The vulnerabilities in Sybil attacks are peer-to-peer, de-centralized. The malicious user gathered many fake identities and pretends in the system. The large fraction of nodes, the malicious user is able to give fake identities. The malicious user is able to give fake identities. Sybil attacks [10], a protocol control the fake influences of Sybil attacks. The protocol is based on social network and edge between two identities represents a true relationship of human established. The risk mechanism in online trading communities, and trust requirement is developing in online. A set of mechanisms [13], reject or reduce the negative effects of behavior. It can be integrated into reputation system. Some difficulties in unfair ratings exists in reputation system, includes unfairly low ratings. A personalized approach [14], handling the unfair rating effectively and increases the centralized reputation system. Trustworthy agents, reduces the difficulties in distributed reputation management.

To represent the evidence [15], and handle the ratings which are given by agent. The local evidence is joins with a evaluating an agent. In reputation system, increasing the difficulties in the selection of member in virtual organizations. The specific model [16], the different reputation models. The path trust algorithm is contributes the majority. The file sharing and distributes information receiving more attention. In ideal environment, the spreading inauthentic files by self-replicating.

B. Yu and M. Singh proposed [15] for agents to function effectively in large and open networks, they must ensure that their correspondents, i.e., the agents they interact with, are trustworthy. Since no central authorities may exist, the only way agents can find trustworthy correspondents is by collaborating with others to identify those whose past behavior has been untrustworthy. In other words, finding trustworthy correspondents reduces to the problem of distributed reputation management.

According to his proposed approach adapts the mathematical theory of evidence to represent and propagate the ratings that agents give to their correspondents. When evaluating the trust worthiness of a correspondent, an agent combines its local evidence with the testimonies of other agents regarding the same correspondent. Experimentally studied this approach to establish that some important properties of trust are captured by it.

A. Josang proposed [16] Virtual Organizations enable new forms of collaboration for businesses in a networked society. During their formation business partners a reselected on an as-needed basis. We consider the problem of using a reputation system to enhance the member selection in Virtual Organizations. According to his proposed solution the use of a specific model of reputation different from the prevalent models of reputation. The major contribution of this paper is an algorithm (called Path Trust) in this model that exploits the graph of relationships among the participants. It strongly emphasizes the transitive model of trust in a web of trust. We evaluate its performance, especially under attack, and show that it provides a clear advantage in the design of a Virtual Organization infrastructure.

The unique global trust value [18], reduce the number of downloads of inauthentic files. The scalable structure [23], represented the travelling wave power divider and combine structure.

III. RELATED WORK

As multiple methods are handle to against the fast development and visible of the reputation system to protecting reputation systems by using the defense schemes. We separated them into three ways.

In the first ways, the defense approaches is provide a certain time period for the user to give the ratings, this approach can identify the attackers from inserting a large amount of dishonest rating through a few user IDs within a short period of time.

In second way, the aim is to increase the cost of introducing an attack and some other schemes is used to increase the cost acquiring diverse user IDs by binding identity with IP address. To detect the network co-ordinates by using a Sybil attacks. This scheme greatly increase the attack cost.

In third way, the defense approaches investigate rating statistics. In this approaches they consider the ratings as the random variable and assume that the dishonest rating have different from normal rating and this approach use the two method to eliminate the dishonest rating that is controlled anonymity and cluster filtering. In forth way of the approach

is to determine the users rating behavior. Such method is to check the user's history and identity the bad and dishonest rating of the user. The malicious user not cares about the normal ratings and then provides the dishonest rating to the items. Fourth scheme, it evaluate the reputation system, this method is used to check the user can give the rating is honestly or not.

In fourth category has approached to investigate the ratings of user's behaviors. Assume this users gave bad rating, this is tend to be provide dishonest ratings. Such type of approaches determines the rating weight based on the reputation of the user's who gives ratings. Such kind of reputation is also known as trust or reliability.

In this work, we proposed a reputation scheme, RAT. The aim of our proposed scheme is (1) to recover the reputation score, the RAT checks the session time (2) it check the rating at the time (3) RAT checks the each and every rating given b y the malicious user. It makes the performance evaluation more efficient and convincing. The models contains in Rate Auditing Techniques are, 1) the client and server communication 2) Reputation system models 3) Implementing RAT technique.

IV. EXISITING WORK

A. overview

The existing TATA scheme consists of two components i) a time domain anomaly detector ii) a trust model based on the Dempster-shafer theory.

TATA achieves a significantly better performance in terms of identifying items under attack, detecting malicious users who insert dishonest ratings, and recovering reputation scores A trust analysis is then conducted based on the anomaly detection results. The concept of user behavior uncertainty from the Dempster–Shafer theory to model users' behavior patterns, and evaluate whether a user's rating value to each item is reliable or not.

The performance of TATA, two other representative reputation schemes, and previously proposed scheme TAUCA is evaluated against real user attack data collected through a cyber competition. TATA demonstrates significant advantages in terms of identifying items under attack, detecting malicious users who insert dishonest ratings, and recovering reputation scores. As diverse manipulations against reputation systems appear and develop rapidly, defense schemes protecting reputation systems are also evolving accordingly. In existing system, TATA scheme contains two components (a) a time domain anomaly detector and (b) a trust model based on the Dempster-Shafer theory.

To detect irregularities by analyzing time domain information. In TATA, sorting the rating in a descending order to a particular time when they are given. Many of the items have intrinsic and stable quality, it should be reflected in normal rating at a time of distribution. The anomaly indicates the rapid changes in the values of rating. TATA anomaly detector detect the small changes occurring in a over time. If the item is triggered and detector, the changes occurring in an intervals. The TATA is used to detect anomaly from a new angle: analyzing time domain information. Specifically, to organize the ratings to a given item as a sequence in the descending order according to the time when they are provided. This sequence, denoted by, actually reflects the rating trend to the given item. In practice, many items have intrinsic and stable quality, which should be reflected in the distribution of normal ratings. If there are rapid changes in the rating values, such changes can serve as indicators of anomaly.

Therefore, the change detector in TATA as the anomaly detector, which takes the rating sequences as inputs and detects changes occurring in the rating sequences. The change detector will detect not only sudden rapid changes but also small changes accumulated over time. In this way, even if malicious users insert dishonest ratings with small shifts to gradually mislead items' reputation scores, such type of changes will still be accumulated and finally be detected by the change detector. If the change detector is triggered by an item, the time intervals in which the changes occur are called change intervals.

The change intervals may still contain normal ratings. Therefore, we introduce the trust analysis module.

- Trust model evaluates the user's reliability separately of different products. Using this reduce the damages which is causing by the malicious users.
- Introducing a user behavior uncertainty trust model based upon the Dempster-Shafer theory could earn high trust value only if it earn a correct amount of observations.

Reputation system architectures figure 1. have an impact on the selection of approaches for handling unfair ratings. There are basically two types of reputation systems in terms of their different architectures, centralized reputation systems and distributed reputation systems . In centralized reputation systems, central servers collect ratings for each provider agent from consumer agents after transactions between them have succeeded. Central servers do not record all of the ratings of each individual consumer agent. Therefore, approaches used in these systems cannot consider consumer agents' personal experience with advisor agents' advice.

The approaches used in centralized reputation systems, such as Iterated Filtering, Cluster Filtering and GM-GC, are based on all ratings of provider agents and belong to the "public" category. Results from those approaches do not differ for different consumer agents. In distributed reputation systems, there is no central location for submitting ratings or obtaining advisor agents' ratings. A consumer agent should simply request advice about a provider agent from advisor agents. Even though some of distributed reputation systems have distributed stores for collecting ratings, it is still costly to obtain all ratings for the provider agent. Therefore, approaches used in these systems cannot consider all agents' ratings for the provider agent.

The approaches used in distributed reputation systems, such as TRAVOS, Bayesian Network and RRSMAN, handle unfair ratings by estimating the trustworthiness of an advisor agent based on each individual consumer agent's personal experience with the advisor agent's advice. These approaches belong to the "private" category. Temporal Analysis - Change Detector In the temporal analysis, we organize the ratings to a given item as

a sequence in the descending order according to the time when they are provided. In many practical reputation systems, items have intrinsic and stable quality, which should be reflected in the distribution of normal ratings.

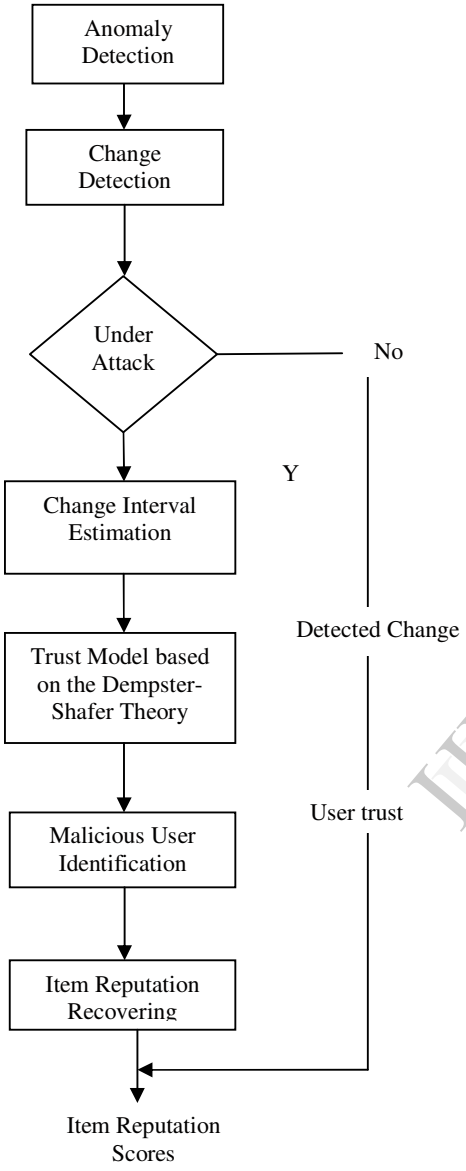

Fig. 1. System Architecture

In fig 1, At last, the low trust values of users will be considered as malicious users and detected target items ratings will be removed. The other ratings are calculate the reputation system.

B. *Temporal Analysis-change detector*

For different application scenarios [20, [21], developed a many change detectors. There is no necessary for a normal ratings follow a particular distribution and using a small bias, the attackers can insert a dishonest rating, so, chose a change detector, it is insensitive to the probability of data distribution and it can be detect the small shift. With the use of CUSCUM detector [21], to build the requirements.

C. *Trust model based on the Dempster- shafer theory*

To find the suspicious users, can provide the ratings during the detected the change intervals. All users are not malicious users because the normal users may provide the biased rating due to human error. To differentiate the normal users and introduced the trust analysis method. The In trust models is used to find the user trust value are determined their good and bad behavior but it is not efficient. Consider two method of calculations. In first calculation the user A has 5 good behavior and 5 bad behavior. In second calculations the user B has a new user so they does not have a behavior history. In many trust model [5],[12], to find the both of their trust values. By Dempster-shafer theory can differentiate these two method. The concept of behavior uncertainty the trust model based upon on the Dumpster-Shafer theory to represent the behavior of the user.

D. *Malicious user identification*

In this method finally, the trust value of each user can be detect. If the users with low trust values they consider as a malicious users, so removing the ratings based upon the low trust values. Detect the user can provide the more number of normal rating and if the user as a malicious user provide the less number of normal ratings. In this method, can identify malicious user based upon the trust values.

E. *Bayesian network system*

In Bayesian reputation systems are quite flexible and can relatively easily be adapted to different types of applications and environments. The advanced feature of Bayesian network is to provide a concise overview of the rich set of features that characterizes Bayesian reputation systems. In particular we demonstrate the importance of base rates during bootstrapping, for handling rating scarcity and for expressing long term trends. Reputation systems take as input ratings from members in a community, and can produce measures of reputation, trustworthiness or reliability of entities in the same community. Bayesian reputation systems are discrete in nature meaning that they normally take discrete ratings such as average or good as input. However, in many situations it is natural to provide input ratings to reputation systems based on continuous measures. This paper describes the principles of discrete Bayesian reputation systems, and how continuous measures can provide input ratings to such systems. The method is based on fuzzy set membership functions.

- Feedback Based Reputation System

In online reputation systems, the goal is create large-scale virtual word-of-mouth networks where individuals share opinions and experiences, in terms of reviews and ratings, on various items, including products, services, digital contents and even other people. These opinions, and experiences, which are called users feedback, are collected as evidence, and are analyzed, aggregated, and disseminated to general users. The disseminated results are called reputation score. Such systems are also referred to as feedback based reputation systems.

F. Security model

a) System Model

The feedback-based reputation system as the system in which users provide ratings to items. This model can describe many practical systems. For example, buyers provide ratings to products on Amazon.com and readers rate social news on Reddit.com. The items in above systems are products and social news, respectively. We consider that each user will provide rating to one item at most once, and the rating values are integer values ranging from 1 to5.In practice, reputation systems often allow users to provide reviews as well. In this, focus on the detection of dishonest ratings.

b) Attack Model

An attacker can controller one or multiple user IDs and each of these user IDs is referred to as a malicious user. Malicious users provide ratings to manipulate the reputation score of items. The item whose reputation score is manipulated by malicious users is called a target item. The ratings provided by malicious users to target items are considered as dishonest ratings.An attack profile describes the behavior of all malicious users controlled by the attacker.

V. PROPOSED WORK

A. overview

The proposed RAT is abbreviated as a Rate Auditing Technique to detect the dishonest ratings which are given by the malicious users. In RAT, we propose to find the irregular ratings. Initially the ratings of a specific items are arranged in a descending orders. If any quick changes occur in the values of ratings, such kind of changes are represented by anomaly. Therefore, we proposed a RAT, which takes the input of the sequences of the ratings and find the changes which is made in the sequences of rating. Rat is not only detect the fast changes occurring in the ratings but also it detect an each and every ratings which are given by the users. Now-a-days, peoples having a habit of waiting an any video in a YouTube. The proposed RAT, checks the ratings in a given video by the users is fully viewed or not. The proposed RAT will detect the each and every rating manipulation RAT is also detect the user is purchased a item after and then he rated or not. Thus by doing this the attacker is also detected and given counter measure to their attacks.

In fig 2, the ratings are from the different systems by the different users. These ratings are gathered in Reputation Systems. The rating are checked by the rate auditing technique whether the ratings are valid means it send to the database otherwise the ratings will be discarded.

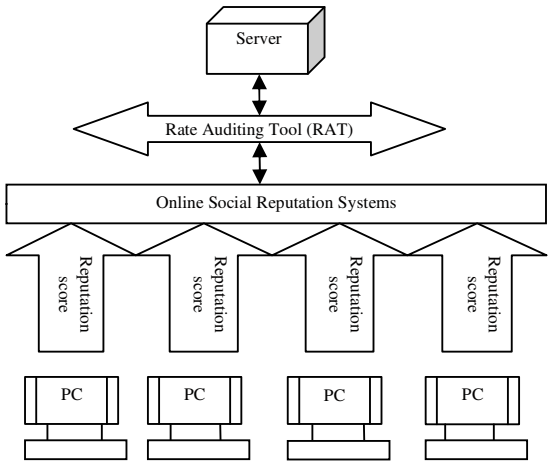

Fig. 2. System Architecture

B. Modules description

In this section, we discuss the models in rate auditing technique. In RAT, we includes three types' modules.

1. *Creating client server communication:*

Server and client systems are established in this module. Client and server form a network with communication channel in between them. Clients can give the request services to the server and the server accepts the request services and then give back the response to the client.

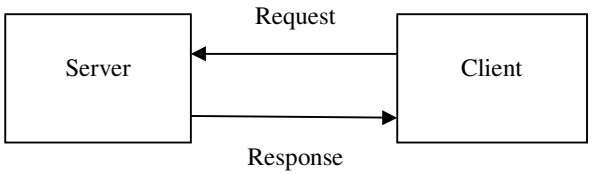

Fig. 3. Creating client server communication

In fig 3. Initally establish the communication between client anr server. Client gave the request to the server and the srever accepts the requests and response to the client.

2. Reputation system model:

Designing a reputation system model which establishes texts, images or videos and publishing them online. In this module , reputation system contains products and their viewing time or product validity will be given by product owner.

In fig 4. Reputation system model establishes the products in the online. Client can view the product and then give the ratings based on the reputation `system. Thse ratings are collected by the server.

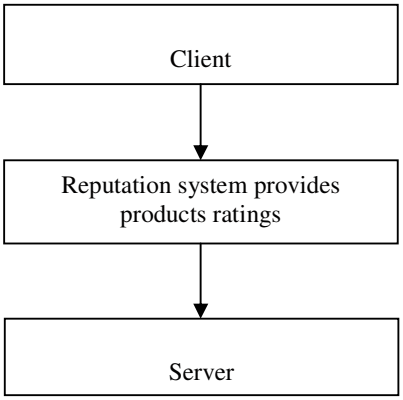

Fig. 4. Reputation System model

3. Rate auditing technique:

In this module, Rate Auditing Technique is implement which is used to determine the reputation score is honest or dishonest. The parameters are developing for this RAT that checks whether the user is authorized or not authorized. If it is found to be given dishonest ratings then that ratings will be rejected. If any attackers try to attack reputation system then that will be given counter attack.

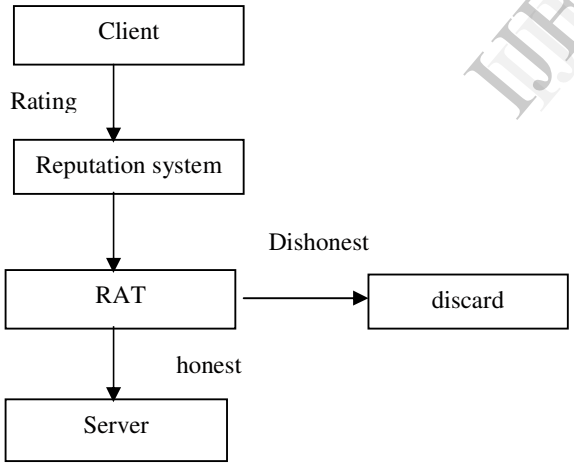

Fig. 5. Implementing RAT

In fig 5 Rate auditing technique used to determine the reputation score is honest or dishonest. the ratings which are found to be honest means it will send to the server otherwise it discard the ratings

VI. PERFORMANC E METRICS

In this section we conduct performance testing of RAT. It is used to determine the reputation score. The fake user's and their details will be determined. Furthermore, the performance of Rate Auditing Technique, in terms of finding the reputation score of the target item can also be determined.

1. Viewing the particular site:

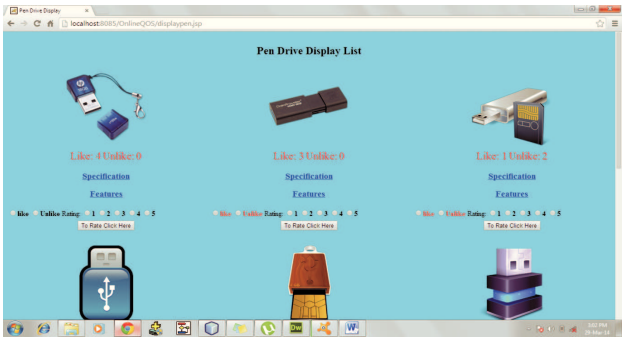

Fig. 6. Viewing the web site

In fig 6, user view the web page normally, but they view the items extra features without the login of the web site.

2. Login into site:

Fig. 7. Login into site

In fig 7. User can give their details and sign into the site. Then, the can be authorized in the site. The user details can store into database, the admin can view the user details.

3. Selecting the user:

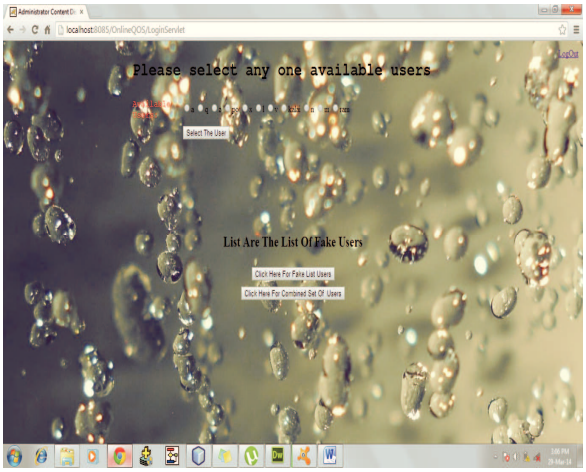

Fig. 8. Selecting the user

In fig 8, if the user provide a ratings means, the admin can check the ratings of the user with RAT. If the

ratings and user behavior is good means he send to the server. It will display on the screen

4. Display user details:

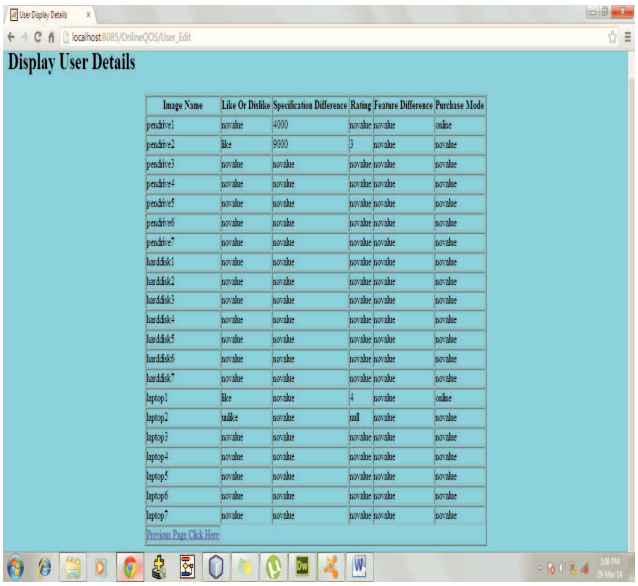

Fig 9. Display user details

In fig 9, display the user details who are all logiin into the web site and give the ratings. Using this details we can identify the fake users.

5. Displaying fake user details:

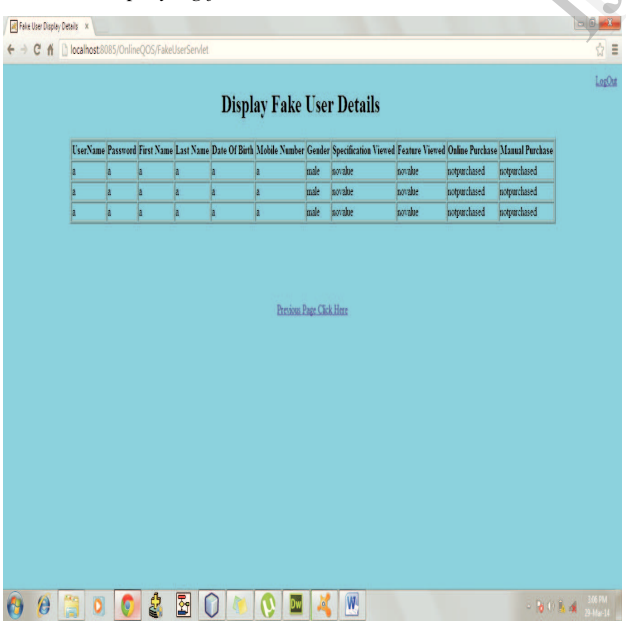

Fig. 10. Displaying fake user details

In fig 10, RAT will determine the fake users who are all can fulfil the conditions and displayed o the admin

6. Combination of the sets:

Fig. 11. Combination of the sets

In fig 11, RAT also determined combination of likes and ratings. It can find the ratings which has to be given by the user. Using this we can identify the hacker,s and fake ratings. The fake ratings will be discarded automatically by the Rate Auditing Techinque.

VII. CONCLUSION

In this paper, we proposed a technique named RAT whicH is the abbreviation of Rate Auditing Technique, which is used to determine the ratings and provide the good reputation score. The proposed RAT is also achieves a better performance in

terms of identify the fake results.

References

[1] Press Relase: Online consumer-generated Reviews have significant impact on offline purchaseBehavior,nov.2007.Available:http://www. Comscore.com/press/release.as? press=1928

[2] R. Lee and H.Paul, use of online Rating systems oct.20,2004[online]. Available: http:// www.pewintment .org/reports/2004/use-of-online-Rating –systems.aspx

[3] Comscore, final pre-christmas push propels u.s.online holidayseason spending throught December 26 to record $30.8 billion dec. 29,2010[online]. Available: http://ir.comscore.com/releasedetail.cmf? releaseID=539354

[4] Buy iTunes rating and comments-Increase iTurnes sales and downloads{online]. Avaliable: http:// www.youtube.com/watch?V= TWV4Xaxco

[5] A. Whitby, A Josang, and J. Indulska, “filtering out unfair rating in Bayesian reputatuion systems” Incfain J.Manage.res., vol.4,no.2,pp.48-64,feb. 2005.

[6] P.Laureti, L.Motet , y-c.zhang, and y-k.yu”Information filtering via iterative refinement,” Europhy. Lett, vol. 75,no.6,pp.1006-1012,2006.

[7] Y. Liu and y.sun,”Anamaly detection in feedback-based reputation systems throught temporal and correlation analysis,” in proc. 2nd IEEE int.conf. Social computing, Aug.2010,pp.65-72.

[8] Y. Yang, Q.Feng, y.sun, and Y.Dai, "Repuataion trap: A powerful attack on reputation system of file sharing p2p environemt," in Proc. 4th Int.conf. security and privacy in communication network, Istanbul, Turkey, sep.2008.

[9] 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.

[10] H. Yu,M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: Conf. Applications, Technologies, Architectures, and Protocols for Computer Communications, 2006, pp. 267–278.

[11] 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.

[12] A. Jøsang andW. Quattrociocchi, "Advanced features in bayesian reputation systems," TrustBus, pp. 105–114, 2009.

[13] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," in Proc. 2nd ACM Conf. Electronic Commerce, 2000, pp. 150–157.

[14] 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. 948 ieee transactions on information forensics and security, vol. 8, no. 6, june 2013.

[15] B. Yu and M. Singh, "An evidential model of distributed reputation management," in Proc. Joint Int. Conf. Autonomous Agents and Multiagent Systems, 2002, pp. 294–301

[16] A. Jøsang, "Trust based decision making for electronic transactions," in Proc. 4th Nordic Workshop on Secure IT Systems, 1999, p. 99-005. [17] J. Sabater and C. Sierra, "Social regret, a reputation model based on social relations," SIGecom Exchanges, vol. 3, no. 1, pp. 44–56, 2002.

[17] S.D.Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks," in Proc. 12th Int. Conf. World Wide Web, May 2003, pp. 640–651.

[18] S. Brin and L. Page, "The anatomy of a large-scale hypertextual web search engine," in Proc. 7th Int. Conf. World Wide Web (WWW), 1998 [Online]. Available: http://dbpubs.stanford.edu:8090/pub/1998-8.

[19] W. A. Shewhart, Economic Control of Quality of Manufactured Product. Princeton, NJ, USA: Van Nostrand, 1931.

[20] E. S. Page, "Continuous inspection schemes," Biometrika, vol. 41, no. 1/2, pp. 100–115, Jun. 1954.

[21] T. K. Philips, Monitoring Active Portfolios: The CUSUM Approach

[22] G. Shafter, A Mathematical Theory of Evidence. Princeton, NJ, USA: Princeton Univ. Press, 1976.

[23] A. Jøsang, "A logic for uncertain probabilities," Int. J. Uncertainty, Fuzziness, Knowledge-Based Syst., vol. 9, no. 3, pp. 279–311, 2001.

[24] Y. Liu and y.L.sun,"Detecting cheating behaviors in cyber comprtitions by constructing competition social network, poster track" in IEEE Intl. Workshop information Forensics and security(WIFS'11), Beazil, Nov.29-Dec.2 2011.