Global Journal of Computer Science and Technology
Volume 11 Issue 11 Version 1.0 July 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

# Predictability Issues in Recommender Systems Based on Web Usage Behavior towards Robust Collaborative Filtering

By P.K.Arunesh, Gopinath ganapathy

*Bharathidasan University Tiruchirappalli, India*

*Abstracts -* This paper examines the effect of Recommender Systems in security oriented issues. Currently research has begun to evaluate the vulnerabilities and robustness of various collaborative recommender techniques in the face of profile injection and shilling attacks. Standard collaborative filtering algorithms are vulnerable to attacks. The robustness of recommender system and the impact of attacks are well suited this study and examined in this paper. The predictability issues and the various attack strategies are also discussed. Based on KNN the robustness of the recommender system were examined and the sensitivity of the rating given by the users are also analyzed. Furthermore the robust PLSA also considered for the work.

*Keyewords :* *component; Recommender systems, security issues, attack strategies, stability of Recommender system.*

*GJCST Classification :* *D.4.8, K.6.5*


*Strictly as per the compliance and regulations of:*

# Predictability Issues in Recommender Systems Based on Web Usage Behavior towards Robust Collaborative Filtering

P.K.Arunesh [α], Gopinath ganapathy [Ω]

*Abstract -* This paper examines the effect of Recommender Systems in security oriented issues. Currently research has begun to evaluate the vulnerabilities and robustness of various collaborative recommender techniques in the face of profile injection and shilling attacks. Standard collaborative filtering algorithms are vulnerable to attacks. The robustness of recommender system and the impact of attacks are well suited this study and examined in this paper. The predictability issues and the various attack strategies are also discussed. Based on KNN the robustness of the recommender system were examined and the sensitivity of the rating given by the users are also analyzed. Furthermore the robust PLSA also considered for the work.

*Keywords : component; Recommender systems,security issues,attack strategies, stability of Recommender system.*

## I. Introduction

Recommendations are generated typically to watch the user navigation behavior as a sequence of pages as visited and they suggest web pages from the opinions and actions of other users with similar tastes and products based on ratings and web sites, and other information besides the actual Information. However, with the rapid growth of the WWW and increasing popularity of the Recommender Systems in e-Commerce sites, they have become susceptible to non veracity, unauthenticated persons and they are unsecured, so it stimulates attacks.

System attack is that the system tries to influence the Recommender System (RS) by injecting biased data into the system. Recently researchers are focusing on this area to design attack models [1], [2], [3] to avoid attacks [4] and to prevent attacks [5]. The important criteria for the current Recommender System researchers are to find whether the recommender systems recommend correct products, items or web sites with out breaching users' privacy and systems authenticity.

An attack on the RS is ascendant by injecting the set of biased attack profiles into the system. Biased ratings data and target products are the contents of each attack profile. Spurious user identities are created by the attacker and the attack profiles injected into the system. Each and every attack can be classified as a push attack or nuke attack.

The performance of the RS has been evaluated widely by accuracy, efficiency, scalability and security. It is difficult to prevent unprincipled users from injecting bogus data into the system. Such insertion of data is referred to as an attack.

The base for the RS is Automated Collaborative filtering algorithm [6]. In our previous work, it has been surveyed the various features of RS [3]. In this paper, the importance of the security issues in recommender systems is examined. [7] shows that user based ACF algorithms are vulnerable to the insertion of biased data and proposed new attack strategy, wherein a recommender system is probed. [1] provides a brief summary of various attack models and their filler strategies.

The high quality of recommendations are maintained by monitoring user ratings and removing shilling attacker profiles from the process of computing recommendations, that is preventing shilling attacks were proposed in [5]. The associated experimental methodologies and the conventional accuracy metrics are given in [8]. The Recommendation Systems are valuable asset to the retail companies and beneficial to the users. Retail companies can help their customers to find things that they want to buy and, in effect, they increase not only sales, but also customer relation and cross-sales. For example, Amazon.com, Netflix and [6] have made recommender systems available to their customers. With recommender systems, there is a natural motivation to promote one's own products to be recommended more often than those of a competitor. So they have to produce quality goods that consumers like and regard highly. But, unscrupulous competitors may opt to take, deceitful route, that they may try to influence recommender system to recommend their products.

It is very easy to see that Collaborative Filtering (CF) is vulnerable to these attacks. User-based CFA collects user profiles. It represents the preferences of many different customers or individuals and it generates recommendations by finding peers with like profiles. If the profile database contains biased data, the

*Author [α] : Department of Computer Science, Sri.S.R.N.M College, Sattur, Tamilnadu, India. Mobile: 91-9443380679, E-mail : arunesh_naga@yahoo.com.*

*Author [Ω] : E- mail : gganapathy@gmail.com.*

recommender system recommends biased recommendations to the genuine users. These effects are precisely found in [9]. How humans fare against RS in predicting items for a user, if the preferences are given, studied in [10]. The accuracy of Recommendation ratings is based on Film Trust web site, a social network determined in [11].

## II. Motivation and Background

Our prior work [12], [13] identifies some of the Recommender system models, Businesses implemented RS and the features were surveyed. All the RS based on web usage mining techniques have strengths and weaknesses. RS have been extensively explored in web mining and the quality, privacy, authentication and security of RS and the user satisfaction with the system are still not optimal. Based on the prior work, it has been found that the commercial RS are not protected. There is a risk in the quality of the predictions. The trust in the consumer for such site can be compromised by attacker. Attackers can inject biased knowledge to the system. So the aim of this work is to address such vulnerability and provide techniques to the service providers to protect their Recommender services from unscrupulous attackers.

## III. Related Works

The vulnerabilities in collaborative filtering RS have been well established theoretically [3]. Attack strategies that are based on creating attack profiles that have similarity with only those genuine users who have already rated the target items are proposed in [1]. Robust collaborative filtering approaches were revived and described the other approaches. They are good in stable shilling [2]. The various attack models and robustness of algorithms were analyzed. The study shows that both user-based and item-based algorithms are highly vulnerable to specific attack models and a novel classification based approach for detecting attack profiles and the effectiveness of neutralizing the attacks evaluated [3]. A classification approach to the problem of detecting and responding to profile injection attacks is described in [14], and the study demonstrates the technique significantly and it reduces the impact of the most powerful attack models.

## IV. Security Issues and Impacts of Attacks

Researches analyse the performance of RS extensively in various dimensions like accuracy, coverage, efficiency, scalability and extensibility. Recently, security of RS has been considered by the research community because it creates many issues in RS and it spoils the efficiency of the RS [4], [7], [8]. Research community identifies that, the RS [9], [10] are operated on open manner and concluded that it is very difficult to protect the RS. Injecting bogus data into the system by the unscrupulous users and spoiling the efficiency of the RS [5], [8].

If a large number of profiles are created, it is a potential drawback of detecting the attack. Remarkable and prominent attack strategies are followed by the attackers. The thorough examination of the RS as means of selected items, by rating a small number of some initial seed items by the RS, the attacker can progressively build up attack profiles which will closely match the distribution of items that have been rated by genuine users of the system, it involves probing the RS.

Since the RS following the voting concept which are based on the collaborative filtering Algorithm, it is easy to attack the target items in the rating distribution. To improve the effectiveness of the attack, the profiles are created, similar to the users who have rated the target items with a lower value or higher value [1]. To improve the similarity, the randomly selected filler items are assigned the average ratings given to the filler items by those users who have rated the target item at the lower scale or higher scale [1].

Various strategies and attack types are followed by the attackers to improve the effectiveness of the attacks. It is a major issue for the RS and obviously there arises the question of security [20].

Random attack, average attack, Bandwagon attack, Segment attack, Love/Hate attack and Reverse bandwagon attack are some of the attack models that threaten the trustworthy Recommender systems [3].

Attacks on Recommender Systems which are implemented by the business using web technologies, can affect the quality of the prediction and suggestions given by the RS, resulting in decreasing overall user satisfaction with the system.

In this paper, the various attack strategies have been examined.

## V. Attacks on Recommender Systems

Researchers proposed various attack models on shilling of RS. Some of the popular attack models focused by the researchers are considered here.

An attack is classified as low-knowledge or high-knowledge attack. More detailed knowledge of the rating distributions of each item present in the system required for high-knowledge but low-knowledge attack depend on the RS for information on the items is minimal to launch an attack. The approach of constructing the attack profiles is based on knowledge about the Recommender Systems, its products, items, rating database and the users of RS.

*a) Profile Injection attack*

Fictitious user identity and target item to be promoted or demoted are the biased rating data associated in each attack profiles that are the attack

against the collaborative filtering recommender systems. A profile-injection attack against RS consists of a set of profiles added to the system by the attacker.

Let U a set of users, P be a set of products, R a set of ratings values, and UF = {uf1, uf2, uf3,…ufn} a set of user profiles, where each $uf_i$ is a set of pairs (i,r), where $i \in I$ and $r \in RU$ {null}, with null representing a missing or undefined rating. The general form of the profiles is given in figure. 1. Each profile is identifying four sets of products singleton target item, set of selected items, set of filler items and set of unrated items [14].

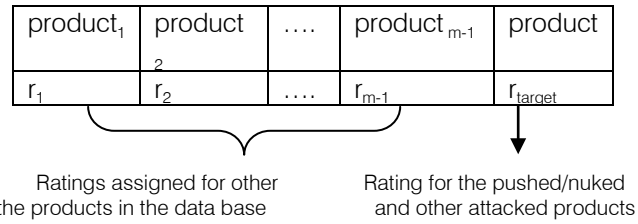


*Fig. 1:* General profile format

On shilling of RS, researchers proposed various attack models. Some of the popular attack models on which much research is focused are discussed below:

***Push Attack and Nuke Attack:*** An attacker may insert profiles to make a product more likely or less likely to be recommended. The possible aim of the attacker might be simple vandalism to make the entire system function poorly.

***Random attack:*** The attack profiles consist of random ratings assigned to the filler items and a pre specified rating assigned to the target item. This is a low knowledge attack. It requires minimal knowledge to obtain the system mean value. This model is not an effective attack [3].

***Average Attack:*** It is most powerful attack model that the filler items are selected randomly and each filler item is assigned its mean rating. Mean rating corresponds to the average rating for the item across all users in the database who have rated it. This is a high-knowledge attack. The ratings of each filler item are required to mount an attack [1].

***Bandwagon attack.*** The aim of this attack is to associate the attack to the small number of frequently rated items that have high popularity among the users. The created attack profiles may have the higher chances of being similar profiles to a large number of users. The target item and the selected items are assigned maximum rating value. This is a low-knowledge attack and the data can be obtained from publicly available information sources.

***Segment attack.*** This attack model is designed to push an item to a targeted group of users who are most likely to be influenced by the recommendation. The segment of users who have similar tastes and features for the particular items, and the group of users who have rated highly for the particular item are identified. So, an attacker who intent to promote an item will try to get his target item recommended to this segment of users as the likelihood of influencing than is higher.

**Love/Hate attack :** This is a very simple attack, and requirement of knowledge is very low. This attack consists of profiles in which the target item is given the minimum rating value.

**Reverse Bandwagon attack :** This is a variation of the bandwagon attack, in which the selected items are those that tend to be rated poorly by many users. These items are assigned low ratings together with the target item. Thus the target items are widely disliked items, increasing the probability that the system will generate low predicted ratings for that item.

*b) Simulation of an attack*

For the purpose of experimentation the publicly available Movie–Lens[1] dataset was used. More than 1,00,000 ratings on 1682 movies by 945 users ratings available in the dataset. One to five are the rating integer values. Where '1' is considered as lowest and '5' is the highest value. In this example around five users rating scale for set of ten movies were considered. Please see Table 1.

A new user, NewUSR having built a profile from previous visits and returns to the system for new recommendation. The set of product (movies) rating pairs are the representations of a user profile. Table 1. shows New users profile along with the five genuine users. Based on using a simplified user based CF approach USR3 and NewUSR have identical tastes and one might want to rate that NewUSR would like to rate 3 to $m_{10}$ because USR3 does.

In order to mount an attach to promote the movie m10, an attacker, has inserted five attack profiles (Atk 1 – 5) into the system. Each attach profile gives high ratings to movie m10, labeled m10. After the attack, attacker Atfk5's Profile is the most similar one to the new user and would yield to predicted rating of 5 for m10. Table 2. illustrates the example.

*Algorithm (1).*

Step.1 For each user

Compute the similarity of ratings with the new user, using the Pearson Correlation from the rating vector.

Let Exx = $\sum(x_i - \bar{x})$, Eyy = $\sum(y_i - \bar{y})$

Compute the Global value of

SExx = $\sqrt{(x_i - \bar{x})^2}$, SEyy = $\sqrt{(y_i - \bar{y})^2}$

Compute the CC = Exx * Eyy / SExx * SEyy

Step.2 Max = the maximum similarity rating in the system

Step.3 For the Sensitivity analysis of users rating, push random data to the user's ratings vector.
Step.4 Repeat Step.1 and 2
Step.5 Find the similarity ratings.
Step.6 Compute the normalized effect of ratings.

Suppose if the system using an product based CF approach, then the predicted rating for $m_{10}$ will be determined by rating vector for $m_{10}$ with those of the other products. In our example rating scale, the predicted rating is 3. The product based and user based collaborative filtering approaches are more robust algorithms can still be are vulnerable (14). Table 2. is an example for push attack, m5 and m10 focused to promote. The Nuke attack is on other side, that the lowest rating 1 is inserted to product M4 to demote the recommendation. From the example, M5 was preferred by many users. In general the aim of the research is to protect collaborative filtering recommenders from the biased data insertion by profile injection attacks.

## VI. Attack Resistant Robust Algorithms

In order to curb attackers, the existing CF algorithm and other models should be redesigned to abate their influence. The researchers found that, the Nearest Neighbor algorithm can be quite sensitive to data manipulation and CF algorithm that carry out recommendations based on a particular class of probabilistic models which are surprisingly robust.

*a) K Nearest Neighbor Algorithm*

The classic KNN user–user and item–item algorithms was introduced in [9] and predicted the ratings for the users and items, several optimizations and parameters were used in [15] and the version of KNN was tested based on the measure of similarity between ratings vectors.

$$S(x, y) = \frac{\sum_{(n:xn\neq 0)}(x_n - \bar{x})(y_n - \bar{y})}{\sqrt{\sum_{(n:x_n\neq 0)}(x_n - \bar{x})^2}\sqrt{\sum_{(n:y_n\neq 0)}(y_n - \bar{y})^2}}$$

Where

$$\bar{x} = \frac{\sum(n : x_n \neq 0)x_n}{|\{n : x_n \neq 0)|}, \quad \bar{y} = \frac{\sum(n : y_n \neq 0)y_n}{|\{n : y_n \neq 0)|}$$

The similarity measure resembles correlations coefficient and is referred as cosine similarity measure [15]

To make this cosine similarity measure as robust to predict the rating of product $M_n$, for n >=3, by a user with past ratings $x^{n-1}$, KNN algorithms identifies a set of neighbors SN as $N(M_n, x^{n-1}, W)$ to be K most similar ratings vectors in W among those that provide ratings for product $M_n$.

The following scalar similarity prediction was generated by the algorithms.

$$SN = \max\{x_{vn}^{-n-1} + \frac{KX \times .SW(w_{vn} - \bar{w})}{KX \mid SW \mid}\}$$

Where $S_{max}$ = max {S:S ε S},

$$\bar{w} = \frac{\sum\{n : w_n \neq 0\}w_n}{|\{n : w_n \neq 0\}|}$$

$$KX = \sum w \in N(v_n, x^{n-1}, W)$$

$$SW = S(w, x^{n-1})$$

*b) Probabilistic Latent Semantic Analysis*

This model [16] is a well known technique for text analysis and used for discovering the hidden relationships between data. The approach was highly successful and popular for indexing documents and it can extend to handle collaborative filtering. The hidden dependencies among users and items in a rating vector can be enabled using probabilistic model in PLSA. Recent studies [2] [17] says that accuracy has been a well known advantage of PLSA and also concluded that PLSA is a very robust collaborative filtering algorithm. Rather than directly computing neighbors, PLSA clusters the users and items then the clusters are used to compute predictions. PLSA is highly stable in the face of shilling attacks. Shilling users are close to many users and they dominant in one cluster due to their extraordinary similarity [18].

PLSA discovering process is, consider the set of n users, U = {$u_1$, $u_2$, $u_3$ … $u_n$) and the set of m items, I = {$i_1$, $i_2$, $i_3$ …. $i_m$}, the model PLSA associates an unobserved factor variable z, with observations the rating data, Z = {$z_1$, $z_2$, …..$z_i$}. The joint probability can defined for the target user u and a target item i.

$$P(u, i) = \sum_{k=1}^{l} \Pr(zk).\Pr(u \mid zk).\Pr(i \mid zk)$$

The maximizing the likelihood L(U.I) of the rating data, the parameters $Pr(Z_k)$, $Pr(U|Z_k)$ and $Pr(i|Z_k)$ has to estimate.

$$L(U, I) = \sum_{u\in U}\sum_{i\in I} r_{u,i} \log \Pr(u, i)$$

where $r_{u,i}$ is the rating of user u for item i.

The standard method for statistical inference, the Expectation Maximization Algorithms (EMA) can be used to maximize the log – likelihood in mixture models like PLSA and parameter estimation. Based on the initial values of

$$\Pr(zk|u,i) = \frac{\Pr(zk) \bullet \Pr(u \mid zk) \bullet \Pr(i \mid zk)}{\sum_{k=1}^{l} \Pr(z_k^{'}) \bullet \Pr(u \mid z_k^{k}) \bullet \Pr(i \mid z_k^{'})}$$

$$\Pr(zk) = \frac{\sum u \in U \sum i \in Ir_{u,i} \bullet \Pr(zk \mid u,i)}{\sum u \in U \sum i \in Ir_{u,i}}$$

$$\Pr(u|zk) = \frac{\sum i \in Ir_{u,i} \bullet \Pr(zk \mid u,i)}{\sum u' \in U \sum i \in Ir_{u,i} \bullet \Pr(zk \mid u',i)}$$

$$\Pr(i|zk) = \frac{\sum u \in Ur_{u,i} \bullet \Pr(zk \mid u,i)}{\sum u \in U \sum i' \in Ir_{u,i} \bullet \Pr(zk \mid u,i')}$$

To reach the local optimum, the expectation and maximization steps are iterated. So it monotonically increases the total likelihood of the observed data L(U, I).

The segments of users, that have similar tastes can be now identified with help of this approach. For each latent variable $Z_k$, a user segment $C_k$ created and all the users are selected based on probability $\Pr(U|Z_k)$ exceeding a certain threshold $\mu$. [19]

| | $m_1$ | $m_2$ | $m_3$ | $m_4$ | $m_5$ | $m_6$ | $m_7$ | $m_8$ | $m_9$ | $m_{10}$ | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $USR_1$ | 3 | 2 | 1 | - | 1 | 2 | 4 | 5 | 5 | 1 | 0.2806 |
| $USR_2$ | 2 | 1 | 2 | 5 | 2 | 1 | 3 | 3 | 3 | 2 | 0.073324 |
| $USR_3$ | 1 | 3 | 2 | 1 | 3 | 3 | 2 | 5 | 3 | 3 | 0.437877 |
| $USR_4$ | 1 | 2 | - | 3 | 4 | 3 | 3 | 4 | 2 | 3 | 0.044014 |
| $USR_5$ | 3 | 3 | 2 | 2 | 1 | - | 3 | 3 | 4 | 2 | 0.334021 |
| New USR | 3 | 4 | 3 | 3 | 2 | 2 | 2 | 5 | 2 | ? | |
| Before | -0.58 | 0.468 | 0.158 | 0.327 | 0.769 | 0.489 | -0.868 | 0.1660 | -0.908 | | |

*Table 1 :* New users profile along with the five genuine users

| | $m_1$ | $m_2$ | $m_3$ | $m_4$ | $m_5$ | $m_6$ | $m_7$ | $m_8$ | $m_9$ | $m_{10}$ | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Atk 1 | 2 | 4 | 3 | 4 | 3 | 5 | 4 | 5 | 4 | 5 | 0.3826 |
| Atk 2 | 3 | 1 | - | 1 | 5 | 2 | | 1 | 3 | 5 | 0.0451 |
| Atk 3 | 2 | 2 | 3 | 1 | 5 | 2 | 3 | - | 4 | 5 | -0.2665 |
| Atk 4 | 3 | 2 | 2 | 1 | 5 | - | 1 | - | 2 | 5 | 0.0984 |
| Atk 5 | 4 | 4 | 3 | 1 | 5 | 2 | - | 3 | 1 | 5 | 0.4875 |
| New USR | 3 | 4 | 3 | 3 | 2 | 2 | 2 | 5 | 2 | ? | |
| After | 0.232 | 0.322 | 0.381 | -0.042 | 0.748 | 0.228 | -0.552 | -0.415 | -0.489 | | |

*Table 2 :* New users profile along with five attackers

## VII. Recommender System Impact Analysis

To evaluate the robustness of the recommender algorithm based on Collaborative Filtering, the sensitivity of the rating vector was tested. In rating vector, the rating given by the users was increased and decreased randomly. Based on this change, the result, affects the recommendations. For example, the user1's rating for m2 was '2' which was increased as '5', the prediction for the New USR was changed. Figure 4 shows the effect of the sensitiveness of the rating vector and we conclude that it is very high sensitive. When there is a change in rating scale randomly. Algorithm (1) describes these steps and please refers Figure 5 for other attack effect sensitiveness.

To analyze the effectiveness of the recommender system, the user's unvoted rating in the rating vector was filled using New Users ratings and the similarity rating was computed based on KNN algorithm. Figure 6 shows the effects. There is no remarkable change in the recommender system. So we conclude that this part of filling in missing ratings will not affect the recommender systems considerably. The algorithm for the predicted vote for the unvoted users rating is described as follows.

Algorithm (2).

Step.1 For each user
Find the rating given by the users rating vector.
$RV(i,j) \leftarrow x, x \geq 1$ and $x \leq 5$.

Step.2 If the rating x is not between the rate, 1 and 5 then
$RV(i,j) \leftarrow Newuser(i,j)$.

Step.3 Repeat the above steps for all the users

Step.4 Compute the similarity ratings based on

step.1 of algorithm(1).

Repeat the computation for all users in the rating vector.

Step.5 Find the maximum similarity with the new user.

Step.6 Compute the normalized effect of ratings.

## VIII. Conclusion

In this paper, the robustness and stability of the Recommender System were surveyed and analyzed. The predictive ability of the recommender System based on collaborative filtering is of high standard and remarkable. But the standard user-user based or item-item based collaborative filtering algorithm has been shown quite vulnerable to profile injection attacks. Attackers are the able personalities to bias recommendations by constructing a number of profiles associated with fictitious identities.

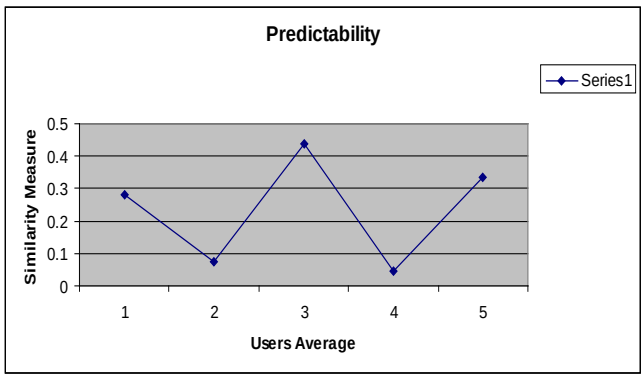


*Figure 4*

Attack prevention and detection, detecting the spam users, preventing attacks and overcoming the attack strategies are still a challenging problem for the research community because a lot of web based recommender service providers provide free access to users via simple registration process. So, it can be exploited by the attackers. They can create multiple identities for the same system and can insert ratings in a manner that affects the robustness of the algorithm or the system.

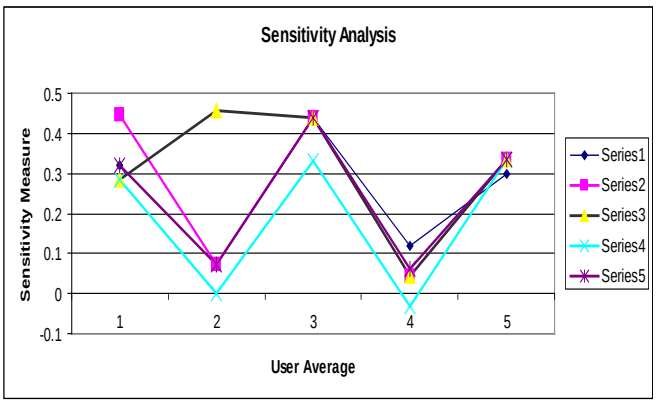


*Figure 5*

Probabilistic Latent Symmetric Analysis is one of the robust Collaborative Filtering algorithms. This work concludes that, its accuracy has been advantage for predictions.

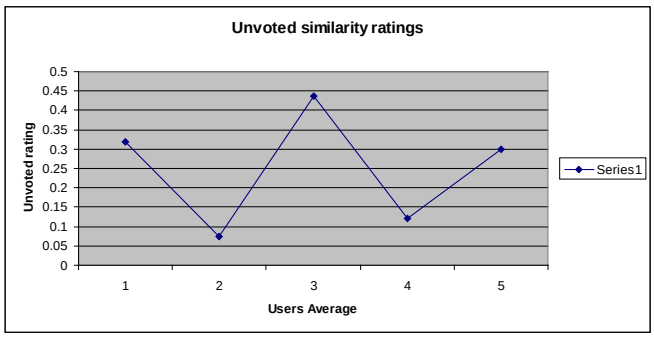


*Figure 6*

Future works include developing principled Recommender system algorithms for web site and web page recommendations based on implicit ratings which are robust and will avoid the behavior in case of attacks.

## References Références Referencias

1. S.Ray and A.Mahanti "Filler Items Strategies for Effective Shilling Attacks", ECAI 2008, PP 31-34.
2. B.Mehta and T.Hofmann, "A Survey of Attack-Resistant Collaborative Filtering Algorithms" IEEE 2008.
3. B.Mobasher, R.Bruke,R.Bhaumik and C.Williams "Toward Trustworthy Recommender Systems: An Analysis of Attack Models and Algorithm Robustness", ACM vol 7, No.4, 2007, pp 23:1-23:38.
4. S.Zhang, A.Chakrabarti, J.Ford and F.Makedon "Attack Detection in Time Series for Recommender Systems" ACM, KDD'06 2006.
5. P.Chirita,W.Nejdl and C.Zamfir "Preventing shilling attacks in online recommender systems" ACM WIDM'05, 2005.
6. Resnick,P.Iacovou, N.Suchak,M.Bergstrom and J.Riedl.1994, GroupLens: A open architecture for Collaborative filtering of netnews, In ACM Proc 175-186.
7. M. O'Mahony,N.J.Hurley and G.Silvestre "Recommender Systems: Attack Types and Strategies", AAAI-05, 2005, PP 334-339.
8. S.McNee, J.Riedl, and J.Konstan "Accurate is not always good: How Accuracy metrics have hurt Recommender Systems" ACM, CHI-2006.
9. S.Lam and John Riedl "Shilling recommender Systems for Fun and Profit", ACM 1-58113-844-x/04/0005, WWW2004, USA, 2004.
10. V.Krishnan, P.Narayanashetty, M.Nathan,R.Davies and J.Konstan "Who Predicts Better?-Results from an Online Study Comparing Humans and an Online recommender System", ACM, RecSys'08, 2008, pp 211-218.

11. J.Golbeck "Semantic Web Interaction through trust Network Recommender Systems" 2005.
12. G.Ganapathy, K.Arunesh "Recommendation System Framework based on Web Usage Mining IJAM vol 22 ISSN 1311 – 1728 No 6 2009.
13. G.Ganapathy, K.Arunesh "Feature Analysis of Recommender Techniques Employed in the recommender engines." Journal of Computer Science 6(7) pp 748 – 755, 2010, ISSN 1549 – 3636.
14. C.A.Williams and B.Mobasher "Defending recommender systems : detection of profile injection attacks" SOCA (2007) 1:157-170, DOI 10.1007/s 1761 – 007 – 0013-0.
15. B.VanRoy and X.Yan "Manipulation Robustness of Collaborative Filtering" working paper 09 – 21 April 1, 2010. www.netinst.org
16. Thomas Hofmann "Latent Semantre Models for Colloborative Filtering" ACM. Vol 22, No.1, 2004, pp 89 – 115.
17. JJ.Sandvig,B.Mobasher and R.Burke "Robustness of Collaborative Recommendation Based On Association Rule Mining" ResSys'07, ACM 2007, pp 105-112.
18. B.Mehta "Unsupervised Shilling Detection for Collaborative Filtering" AAAI, 2007, pp 1402-1407.
19. B.Mobasher, R.Burke and JJ.Sandvig " Model-Based Collaborative as a Defense Against Profile Injection Attacks" AAAI 2006
20. M.P.Mahony,N.J.Hurley and G.C. Silvestre, "Recommender Systems: Attack Types and Strategies"AAAI 2005-p.334-339

This page is intentionally left blank