DETECTION AND PREVENTION OF MALICIOUS FEEDBACK IN WEBSERVICE

Rajeswari V1, Kalaivani C2, Divya B3, Anandraj P4

1 Student, Department Of Computer Science And Engineering, EGS Pillay Engineering College, Nagapattinam, India
2 Student, Department Of Computer Science And Engineering, EGS Pillay Engineering College, Nagapattinam, India
3 Student, Department Of Computer Science And Engineering, EGS Pillay Engineering College, Nagapattinam, India
4 Assistant Professor, Department Of Computer Science And Engineering, EGS Pillay Engineering College, Nagapattinam, India

ABSTRACT
Web service recommendation systems can help service users to locate the right service from the large number of available Web services. Avoiding unfair feedback is a fundamental research problem in the design of Web service recommendation systems. Reputation of Web services is widely-employed metric that determines whether the service should be recommended to a user. The service reputation score is generally calculated using feedback ratings. Existing user feedback rating often leads to degrades the performance of reputation system. In this paper, we propose a novel reputation measurement approach for Web service recommendations. first step is detect malicious feedback ratings by Cumulative Sum Control Chart, and then we reduce the effect of user feedback preferences employing the Pearson Correlation Coefficient. Moreover, in order to avoid malicious feedback ratings, we move for a malicious feedback rating prevention scheme known as Bloom filtering to enhance the recommendation performance. These experiments are conducted by apply a real feedback rating dataset contain 1.5 million Web service invocation records. The experimental results reduce the deviation of the reputation measurement and enhance the success ratio of the Web service recommendation.

Index Terms— feedback rating, reputation, Cumulative, Pearson Correlation Coefficient, Bloom filter

I. INTRODUCTION
World Wide Web is increasingly being used for communication between applications. The programmatic interfaces made available over the web for application-to-application communication are often referred to as web services. There are many types of applications that can be considered web services but interoperability between applications is enhanced most by the use of familiar technologies such as XML and HTTP. These technologies allow applications using differing languages and platforms to interface in a familiar way.

XML and HTTP
XML and HTTP are the foundation for calling web services with Web Services Link. A user interacts with the web service interfaces by sending XML messages over HTTP. XML and HTTP are useful for creating and sending messages because they are flexible and widely supported on many platforms and languages. This interoperability allows applications to communicate using differing languages and platforms using these common technologies. Web Services Link supports XML 1.0 and HTTP 1.1. The XML functionality is supplied by the XML capabilities.

SOAP
Because XML and HTTP are so flexible, a web service message may be represented and communicated in many different ways. Therefore, it is important to have standards that are common among all platforms and languages that use a web service. Simple Object Access Protocol (SOAP) is one standard that formally sets the conventions governing the format and processing rules of XML messages and how they are used with HTTP. Web Services Link supports SOAP 1.1. Online shopping behavior (also called online buying behavior and Internet shopping/buying behavior) refers to the process of purchasing products or services via the Internet. The process consists of five steps similar to those associated with traditional shopping behavior (Liang and Lai 2000). In the typical online shopping process, when potential consumers recognize a need for some merchandise or service, they go to the Internet and search for need-related
information. However, rather than searching actively, at times potential consumers are attracted by information about products or services associated with the felt need. Then they evaluate alternatives and choose the one that best fits their criteria for meeting the felt need. Finally, a transaction is conducted and post-sales services provided. Online shopping attitude refers to consumers' psychological state in terms of making purchases on the Internet.

II. OVERVIEW OF OUR APPROACH

This paper presents a large-scale measurement study and analysis of the structure of multiple online shopping website feedback. Reputation plays a major role in order to choose the right product. So, this paper extends the idea to detect the unfair user and block them further.

Figure 1: overview of our approach

Customer purchase the product, based on the worth to the product user’s deliver their suggestion as a feedback rating are predicted by positive and negative. CUSUM chart are the method used to detect the user’s rating and reduce the effect of user feedback preference by correlation co-efficient and further avoid it by filter.

III. PROPOSED METHODOLOGY:

To address the weaknesses of existing system, this paper extends our previous work by proposing a reputation measurement approach to reduce the deviation of the reputation measurement of services and to improve the success ratio of the service recommendation. Moreover, to prevent malicious users from suppressing benign feedback ratings, this paper presents a malicious feedback rating prevention scheme. This paper makes the contributions: 1) we adopt the Cumulative Sum Control Chart to identify malicious feedback ratings to lessen the influence of malicious feedback ratings on the trusted reputation measurement; 2) we devise feedback similarity computation to shield the different preferences in feedback ratings of users using the Pearson Correlation Coefficient; 3) we propose a malicious feedback rating prevention scheme to prevent malicious users from suppressing benign feedback ratings using a standard Bloom filter; 4) we validate our proposed malicious feedback rating prevention scheme through theoretical analysis, and also evaluate our proposed measurement approach experimentally.

i) Training Algorithm:

Step 1: Select the number of features, n, for the complete system.
Step 2: Train with Username with multiple ratings for same product.
Step 3: Train with IP address with multiple ratings for same product.
Step 4: Perform feature selection specific to each layer.
Step 5: Plug in the trained models sequentially such that only the connections labelled as normal are passed to the next layer.

ii) Testing Algorithm:

Step 6: Test the instance and label it either as attack or normal.
Step 7: If the instance is labelled as attack, block it and identify it as an attack represented by the layer name at which it is detected. Else pass the sequence to the next layer.
Step 8: Block the user for further unfair ratings.

PSEUDO CODE REQUIREMENTS:

MAIN
Begin
PRODUCT_SEARCH()
Get Product
Stop
PRODUCT_SEARCH()
Begin
Var char PRODUCT_NAME, CH F:
do
Write " Input Product name:"

6
Read PRODUCT_NAME
Search for Product in inventory
If Product found
Write
PRODUCT_NAME,
ITEM,B_NAME,P_PRICE,P_IMAGE,QUANTITY
If STOCK<>0 AND Purchase is feasible
Add product to cart
End if
Else
Goto F
End if
Write " Add another product?(y/n)"
Read CH
while(CH<>'n' OR CH<>'N')LOGIN()
End
LOGIN Begin
Varchar EMAIL_ID, ID, PASS, NAME, DOB, AGE, ADDRESS, MOBILENO
If customer has account
E:
Read ID, PASS
If USER_NAME==LOGIN_ID AND PASS==LOGIN_PASS
PRODUCT
Else
Read EMAIL_ID
If EMAIL_ID present in database
Send LOGIN_PASS to Email address
Goto E
End if
End if
Else
G:
Read NAME, DOB, AGE, ADDRESS, MOBILENO, LOGIN_ID, LOGIN_PASS, EMAIL_ID
If LOGIN_ID already present in database
Goto G
Else
Create new account and store details in database
Goto E
End if
End if
End
Product()
Begin
Finalise Products
I:Read LOCAL_ADRS, PINCODE, CNTRY, CONTACT_NO
G:If PIN,CNTRY,CONTACT_NO ARE VERIFIED
H:If mode of payment is CARD
Read CARD_NO, CARD_NAME
End else if
If details verified
Conduct Transaction
Email Customer transaction details
Else
Goto H
Else
Goto I
End
This workplan can be divided into four phases:

1. Recommendation System Module
2. Reputation Measure Module
3. Data Collection Module
4. Malicious Rating Prevention

Recommendation System Module:
In this module, the login page are created ,user are need to enter their username and password.if it is a new user,new user need to create their account to sign in.In the shopping website page,user choose purchasing product displayed in the home page.In order to purchase,user need to use credit card to purchase the item. In this module, user buy the product and deliver their suggestion as feedback.

Reputation Measure Module:
In this module user buy the product and deliver their suggestion as feedback.the feedback is in form of rating.usero rating considered as the major role in the purchase of product.
In online shopping reputation measure.user rating plays a vital role. In order to validate the product sometimes the unfair rating may lead to bad opinion.
In this module/user rating are collected as a file and secure it.

Data Collection Module:
In this module, the entire user profile are collected as a file. That file contain user ID, ip address duration and rating values ip address are help to known the malicious user.
The unfair user are determine by rating over the period time.The rating determine by graph analysis.
The same user who gives the positive feedback as well as negative feedback for same product are identified.

Malicious Rating Prevention:
The identified Malicious rater’s are have to block by IP address, and filter them out to prevent the anomalous feedback rating.The blocking are done by bloom filter. Admin has the responsibility to block the malicious feedback
III. CONCLUSION

The proposed reputation measurement approach utilizes malicious feedback rating detection and feedback similarity computation to measure the reputation of Web services. The efficiency of our proposed approach is evaluated and validated by the theoretical analysis and extensive experiments. The experimental results show that our proposed approach can accomplish a trustworthy reputation measurement of Web services and greatly improve the service recommendation process. The proposed prevention scheme can identify the IP addresses with the offending feedback ratings and block them using a standard Bloom filter. The theoretical analysis indicates the efficiency of the proposed prevention scheme in blocking malicious feedback ratings within the Web service recommendation system. Our on-going research includes investigating the parameters of sampling interval according to the number of feedback ratings, the number of sampling, duration and storage space, and constructing a common malicious feedback rating prevention scheme for Web service recommendation systems.

IV. REFERENCE

Shangguang Wang, Member, IEEE, Zibin Zheng, Member, IEEE, Zhengping Wu, Member, IEEE, Fangchun Yang, Member, IEEE, Michael R. Lyu.


Rajeswari V Pursuing b.e computer science and engineering in EGS pillay engineering college, Anna University.

Kalaivani C Pursuing b.e computer science and engineering in EGS pillay engineering college, Anna University.

Divya B pursuing b.e computer science and engineering, EGS pillay engineering college, Anna University.
Anandraj P received undergraduate and postgraduation degree in Computer Engineering from Anna University in India and having 7 years of teaching Experience.