INTERNATIONAL JOURNAL OF
RESEARCH IN COMPUTER
APPLICATIONS AND ROBOTICS
ISSN 2320-7345

PRECAUTIONARY MEASURES FOR FORBIDDING SOCIAL AND POLITICAL ISSUES THROUGH SOCIAL NETWORK

BL. Aarthi [1], S. Karthik[2], Sharmila. V[3]

[1]ME in KRISHNASAMY COLLEGE OF ENGINEERING & TECHNOLOGY, Cuddalore, Tamil Nadu
Email-id: aarthibhairavacademy@gmail.com
[2]HOD/ASSOCIATE PROFESSOR in KRISHNASAMY COLLEGE OF ENGINEERING & TECHNOLOGY, Cuddalore, Tamil Nadu
[3]ME in KRISHNASAMY COLLEGE OF ENGINEERING & TECHNOLOGY, Cuddalore, Tamil Nadu

Abstract: - There are number of social networking services and loads of usage at present condition. Social networking provides both advantages and disadvantages. People utilize social network only for communication purpose. Twitter is one of the commonly used social media between short times it gained a worldwide popularity. More than 350 millions of posts are tweeted per day. The major drawback of existing is that in twitter the tweets are publicly visible and the tweets can be visited by anyone via commented. So twitter does not provide privacy and security. The networking issues have become a matter of serious concern. The user feels insecure while using twitter as it shares all the personal information in common with third parties. In our proposed system we use Natural language processing (NLP) to identify malicious feedback ratings. NLP acts as a detecting technique which detects the negative or malicious comments and also blocks the abused or negative comments stopping it from sharing the personal details to the public blog.

Index Terms: - Natural Language Processing (NLP), malicious feedback detection

1. Introduction

Twitter is used as a great tool for twitting messages and sharing some universal related topic or discussions it is also used for expressing feelings. Twitter when focussed in business purpose it is very useful. But when it deals with confidentiality it lacks stability. Twitter while considered as a great business platform consumes more help in official usage. By using twitter a large group of communication is available and target markets are insured which is useful for the business clients to develop or exaggerate their business. In other side twitter is the first site that allows spammers. Each spammer should be identified, weed out and filtered from the list time to time. The spammer in the twitter may enter the site and misuse the shared data of other users. They may also pass negative comments and spread malicious feedback [1].

A balanced stage should be maintained with getting friendly with your followers. When this exceeds may cause major problem and ends in negative commenting and abused words. This happens often in twitter. For instance, consider A and B who shares posts or tweet some information regarding politics or post tweets commenting movies. In that case a quarrel or fight may occur between the two. This causes disturbance to other user who view the comments. There are 90% of chances for other user to publicise the fight and comment about it in comment. This promotes a hypothetical state and the state is unavoidable.

In existing system bloom filter where used to find malicious feedback rates and prevent it from abusing comments and attacks. The abusing comments are measured and rated in success ratio recommending the service. This checks the comments of the web service which in turn is employed metric and investigates whether to be recommended to the user or not. Then, the metric sends an authentication that the comments delivery for you is abused. Then the user may tend to erase the comments [2]. This method may not help in all times. If the authentication delivered the results in the delay or corrupted this may affect the user details.

ACS (abusing comment system depends on previous information establishing bond among unknown user. ACS of web services is a issue that no history of new comers is present. In twitter there may be fake tweets and fake addresses which allocate malicious feedback to other users. Malicious feedback in twitters is a preferable assessment of an attribute described on single entity relating observations causing problems. More than one source are simulated deriving abused comments. A reference to aggregated perception is ensured allowing the service requesters for providing abusing comments [3]. Web Service recommendation systems can be employed to recommend the optimal Web service for satisfying user's requirements.

Service recommendations are helpful for users when two or more Web services have the same functionality but different Natural language processing (NLP) performance. NLP is defined as a set of non-functional properties, including Abusing comments, response time, reliability, etc. When multiple Web services formulated AC provides the same functionality, then a feedback rating requirement can be used as a secondary criterion for service selection. Language processing is a set of non-functional attributes like service response time, throughput, reliability, and availability. Service computing are used with multiple and separate systems adopting several business domains as a package functionality suiting routines [4]. While using twitter the privacy is in jeopardy only because of the social media which affects the pride of a person.

2. Evaluating malicious feedback/Abuse comments detection:

Malicious feedbacks are rated accordingly with ACS (abusing computing system). ACS acts as a detecting sector in which the comments are rated and measured. The comments tweeted are separated as division.

The abused and malicious feedback can be classified by measuring:

- Positive feedbacks
- Negative feedbacks

In twitter the feedback ratings are calculated by identifying the indications. The indications are simultaneously recruited and verified. Abusing comments are boots trappers that access newly deployed services. The rating defines a theoretical analysis in which measurements are profiled. The reputation feedback is also measured alternative ways [5].

If it shows positive indication then the comments are positive and the feedback is in stable condition. There is no need for any malicious prevention in this stage of indication.

If it indicates negative indication then the comments are negative and the feedback is not in a stable condition. In this stage there is need of security and privacy protection.

- **Public Tweets** PT (the default setting) PT is a default setting which are visible to anyone, whether or not they have a account. They do not consider any followers or do not calculate the user needs. In public tweets the comments flow are also publicized [6].
- **Protected Tweets** may only be visible to your friends and approves only Twitter followers. Only particular users are granted permission to follow the tweets we post. If others try to interrupt an

indication to admin will be delivered and the admin may block that particular user tweet ID and details [7].

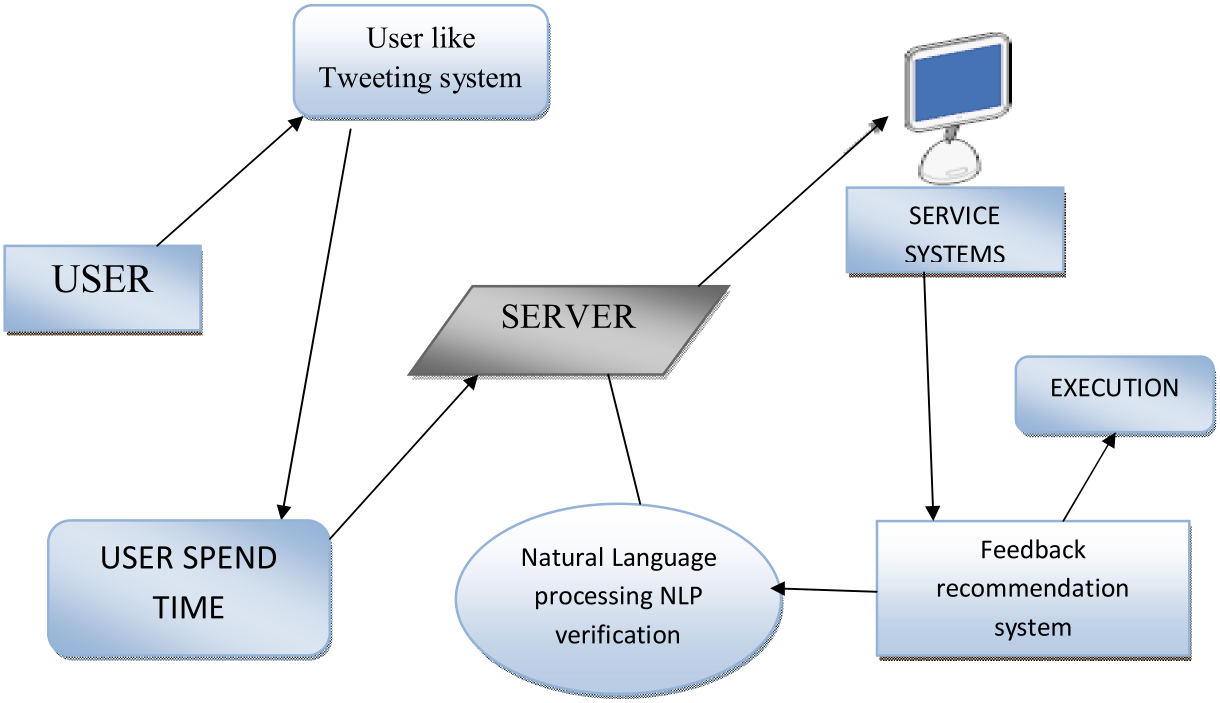
User like Tweeting system
USER
SERVER
SERVICE SYSTEMS
EXECUTION
USER SPEND TIME
Natural Language processing NLP verification
Feedback recommendation system

Fig 1.1 Architecture Diagram for Malicious Feedback Rating

The proposed solutions employ different techniques measuring Web service reputations based on user feedback ratings regarding abusing words or comments. We validate our proposed malicious feedback rating prevention scheme through theoretical analysis, and also evaluate our proposed measurement. A reputation derivation model had also been proposed to aggregate feedbacks into a reputation value that better reflects the behaviour of the service at selection time. The proposed method reduces the abnormality of the reputation measurement. The success ratio of the web service recommendation can be improved [8].

In service-oriented environments where honest and malicious service providers co-exist, finding the exact balance between fairness and accuracy for abusing comments bootstrapping is non-trivial. For instance, a malicious service provider may attempt to clear its (negative) Abusing comments history by discarding its original identity and entering the system with a new one. In contrast, a service provider may be entering the system for the first time without any malicious motives [9]. This can also be avoided and protection can be provided.

3. Natural language Processing (NLP) as malicious feedback detector

Natural Language Processing is defined as a language detector otherwise known as malicious feedback detector. The detector is used to identify the abusing comments provided by other crackers. NLP acts as a language processing detector. NLP at first trace for harsh or abusing comments it validate through indication meter. In indication meter if the indication points to positive then the comments validated are positive so the server allows the comments to be posted. If the indication points towards negative sign then there is detection of abused word usage. In that case the server will be blocked the particular comment is kept for verification in the main server. If the admin allows/permit then the verification is done again and the particular comment is revaluated [10]. But in this process it never allows the comment to pass through or to be posted. Steps followed in detection of malicious feedback/abusing word.

a) Indication check: Check for the indication positive allows user to post comment. Negative indication then do not permit user to post the malicious feedback.
b) Admin verification: At once when the malicious feedback is detected pin point the comment. Picks out the abusing comment sent to main server for Admin verification.
c) Provision to permit: the abusing comment is detected through NLP and the language processing transfers automatically to admin for verification not allowing the server to tweet the abusing comment/post in the twitter.
d) Block the post: if the doubt is clarified and the comment is abused then at once the admin block the post/malicious feedback from the user. The admin also pick out and block or mark list the particular user from twitter.

By this the malicious feedback will not be posted. This protects the other user from quarrel and fights. When the abusing comment or malicious feedback is blocked there won't be any problem occurrence relating the feedback [11].

4. Conclusion:

The service comment (positive & negative comments) score is usually calculated using feedback ratings provided by users. Although the reputation measurement of Web service has been studied in the recent literature, existing malicious and subjective user feedback ratings often lead to a bias that degrades the performance of the service recommendation system. In this paper, we propose a safer comment passing for twitter by using Natural language processing (NLP) measurement approach for Web service recommendations. In this proposed system the feedback measurement in the twitter approach utilizes malicious feedback rating detection and also feedback similarity computation to measure the reputation and harmful quarrel ob web services in common. The prevention scheme can also identify the IP address with abusing/offending comment ratings and block them using the NLP [12]. NLP as a detecting technique finds the wrong comment and transact the comment to admin for verification. And blocks the abusing feedback ratings inside the user web recommended system and protect the user.

5. Future enhancement

Our ongoing research includes extending of storage space and provides lots of memory. And it also includes a common constructing malicious feedback rating for all other web recommended systems [13].

REFERENCES

[1] X. Chen, X. Liu, Z. Huang, and H. Sun. Region KNN: A scalable hybrid collaborative filtering algorithm for personalized web service recommendation, In Proceedings of the 8th IEEE International Conference on Web Services (ICWS'10), pages 9- 16, 2010.
[2] Z. Zheng and M. R. Lyu. Collaborative reliability prediction of service-oriented systems. In Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering (ICSE'10), pages35-44, 2010.
[3] E. M. Maximilien and M. P. Singh. Conceptual model of web service reputation. SIGMOD Record: 31(4): 36-41, 2002.
[4] Z. Malik and A. Bouguettaya. Evaluating rater credibility for reputation assessment of web services. In Proceedings of the 8 th International Conference on Web Information Systems Engineering (WISE'07), pages 38-49, 2007.
[5] Z. Xu, P. Martin, W. Powley, and F. Zulkernine. Reputation enhanced QoS-based web services discovery. In Proceedings of the IEEE International Conference on Web Services (ICWS'07),pages 249-256, 2007.
[6] D. Ardagna and B. Pernici. Adaptive service composition inflexible processes. IEEE Transactions on Software Engineering, 33(6): 369-384, 2007.

[7] W. Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K.Nahrstedt. A trust management framework for service oriented environments. In Proceedings of the 18th international conference on World Wide Web (WWW'09), pages 891-900, 2009.

[8] S. Nepal, Z. Malik, and A. Bouguettaya. Reputation Propagation in Composite Services. In Proceedings of the IEEE International Conference on Web Services (ICWS'09), pages 295-302, 2009.

[9] R. Jurca, B. Faltings, and W. Binder. Reliable QoS monitoring based on client feedback. In Proceedings of the 16th international conference on World Wide Web (WWW'07), pages 1003-1012, 2007.

[10] N. Limam and R. Boutaba. Assessing Software Service Quality and Trustworthiness at Selection Time. IEEE Transactions on Software Engineering, 36(4): 559-574, 2010.

[11] J. R. Douceur. The Sybil Attack. In Proceedings of the First International Workshop on Peer-to-Peer Systems (IPTPS'01), pages251-260, 2002.

[12] F. Li, F. Yang, K. Shuang, and S. Su. A Policy-Driven Distributed Framework for Monitoring Quality of Web Services. In Proceedings of the IEEE International Conference on Web Services (ICWS'08), pages 708-715, 2008.

A Brief Author Biography

BL. AARTHI

aarthibhairavacademy@gmail.com

BL. AARTHI is presently pursuing her M.E degree in computer science and Engineering from Krishnasamy college of engineering and Technology, Cuddalore, TamilNadu, India. She has received her B.Sc. Computer Technology (B.Sc., CT) degree in Computer Technology from Bannari Amman Institute of Technology (BIT), Erode, TamilNadu, India in 2009, M.C.Afrom Coimbatore Institute of Technology (CIT), Coimbatore, TamilNadu, India in 2012. Her research interests are in the areas of Big-data and Image Processing.

S. KARTHIK

S. KARTHIK Completed his B.E. (CSE) degree in the year 2005, M. Tech (CSE) degree in the year 2007, MBA (HRM) in the year 2008, M. Phil (CSE) degree in the year 2009. Currently he is pursuing Ph.D. in the area of Image Processing. Currently he is working as a HOD/ Associate professor in Computer Science and Engineering at Krishnasamy College of Engineering & Technology, Cuddalore, Tamil Nadu, India. His Teaching experience is 10 Years. Previously he worked at GanathipathyTulsi's Engineering College, Vellore, Tamil Nadu, India. His research interests lies in the areas of Image Processing, BIG DATA, DBMS, Data Mining, Data warehousing, Cryptography & Network Security, and Cloud Computing. He has published 7 International Journals and 3 research papers in National/ International conferences. Also he is life member of Indian Society of Technical Education of India (ISTE). He attended many workshops & National seminars in various technologies and also attended Faculty Development Programme.

V. SHARMILA

V. SHARMILA is presently pursuing her M.E degree in computer science and Engineering from Krishnasamy college of engineering and Technology, Cuddalore, TamilNadu, India. She has received her B.E degree in C.S.E from IFET College of Engineering, Villupuram, TamilNadu, India in 2013. Her research interests are in the areas of Image Processing and Big-data.