International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Trust Management in E-commerce Websites

Swati Mahajan[1], Sarika Mahajan[2], Shubhangi Jadhav[3], Sangita Kolate[4]

[1,2]Computer Engineering, SPPU University, Kondhwa, Pune, India
[3]Computer Engineering, SPPU University, Uruli Kanchan, Pune, India
[4]Computer Engineering, SPPU University, Saswad, Pune, India
[5]Professor S. N. Shelke, Dept. of Computer Engineering, Sinhgad College, Maharashtra, India

---

Abstract - *The Benefits of Online Shopping is that it is more flexible and also save lot of time of the customer. By checking reviews of product customer can decide whether to buy the product or not. It also helps the manufacturers to analyze which product is mostly purchased by the user so that they can increase the productivity. Sometimes the customer is not satisfied with the product and gives feedback based on his/her experience. And that comments helps manufacturer to focus on updating product so that it will increase overall productivity. Our system analyzing reviews and the result is shown in graphical representation i.e. either in bar charts or line charts or pie charts so it becomes easy for the customer to understand user's opinion about the particular product. But there are some customers who intentionally gives false feedback which can be positive or negative in order to either increase or decrease the product rating. That's why our focus is to identify and remove such false feedbacks. So, in this paper, we are defending our system against collusion attack and Sybil attack.*

Key Words: Opinion Mining, Opinion Word, Opinion Target, Topic Association, Sybil attack, Collusion attack

1.INTRODUCTION

Nowadays, multiple users are buying products online instead of going into the stores which save their time and they get the flexibility also. The user tracks the product's quality which is given in rating(in the form of stars). So that, customer decide whether to buy the product or not. But, in today's E-commercial websites just giving the overall ratings for the product is not sufficient. Thus, we need to analyze reviews Attribute wise (Topic association) and then display the result for the particular attribute of product (e.g. camera, processor, ram these are different attributes of a mobile phone).

In our proposed system the user has to select the category of the product among multiple categories then he again need to choose a subcategory, assume that there are three categories Books, Electronic Product, Cloths, among these three if one user selects Electronic Product. In Electronic Product there is also another subcategories e.g. Mobile and Tablet, Laptop, Washing Machine, so among

these three subcategories user again has to choose one of them. Again in subcategory user has to select brand e.g. Samsung, Motorola. Samsung which was organized in the database already by the use of hierarchical database model and for that product user can give the review also.

For example, if the user gives feedback as:

"The screen and picture quality of the Oppo mobile phone is the Best"

The admin extracts the opinion targets and opinion words of the reviews given by the user. In this example, Opinion target is screen and picture quality and Opinion word is Best. The system will calculate the percentage according to Good Word's Count and calculates the overall percentage based on which has been calculated previously. The system shows the attribute wise rating as well as an overall rating of the product in the graphical format. The benefit of the Topic Association is that if some users are unaware of the Latest product's features, then that users can also find whether it is good or not through the attributes provided by our system.

If the same user is trying to give a false opinion about the product multiple times from the same machine using the same user account then it is called as Collusion attack.

If the same user gives a false opinion about the product from the same machine using the different usernames then it is called as Sybil attack. So this type of attack can be identified by IP address. The vendor or manufacturer has to take some action against such users. Our system provides the facility to the administrator for deleting such type of reviews and users.

2. LITERATURE SURVEY

Trust management is one of the most challenging issues for the adoption and growth of cloud computing [1].

The highly dynamic, distributed, and non-transparent nature of cloud services make the trust management in cloud environments a significant challenge [2], [3], [4], [5].

In reality, it is not unusual that a cloud service experiences malicious behaviour (e.g., collusion or Sybil attacks) from its users. Protecting cloud services against their malicious users (e.g such users might give misleading feedback to disadvantage a particular cloud service) is a difficult problem [1].

The Sybil attack is an attack wherein a reputation system is subverted by a considerable number of forging identities in peer-to-peer networks means an adversary creates a large number of false/fake/Duplicate identities (Sybil identities) [9].

Sybil attacks can be avoided by using trusted certification. Trusted certification usually relies on a centralized trusted authority for assigning and verifying identities. Sybil accounts in online social networks are used for criminal activities such as spreading spam or malware stealing other users' private information and manipulating web search results. Preventing Sybil attacks is quite challenging [9]. Such an attack arises when malicious users exploit multiple identities [6], [7] to give numerous misleading feedbacks (e.g., producing a large number of transactions by creating multiple virtual machines for a short period of time to leave fake feedbacks) for a self-promoting or slandering attack [1].

3. SYBIL ATTACK

Sybil attacks, where a single entity emulates the behaviour of multiple users. A Sybil identity can be an identity owned by a malicious user, or it can be a bribed/stolen identity, or it can be a fake identity obtained through a Sybil attack. In Sybil attack, a single malicious user creates a large number of peer identities called Sybil's.

In the e-commerce websites like Amazon, Snapdeal, Flipkart, the malicious users are trying to give the reviews (which are fake) on products intentionally, for increasing or decreasing the product's ratings, sales. The malicious user gives the feedback through the single machine (acts as a virtual) from different user accounts just to increase the count of review means it is pretending like multiple user entities. But, the IP address of such user will be the same. So, with the help of Sybil attack, our system will keep the track of such users and the manufacturer can delete such user's accounts from their websites.

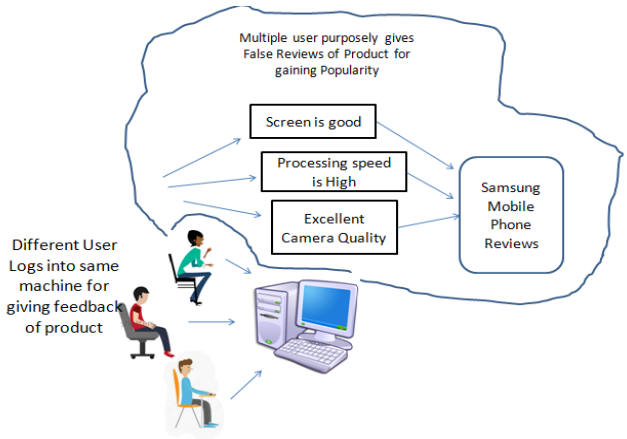

Fig -1: Sybil Attack

In this diagram, multiple users collaborates together to give the false feedback about the product but from the same machine. Here, one user given the feedback as "Screen is good", second user given review as "Processing speed is high" and third user given the feedback as "Excellent camera quality" about the same product Samsung Mobile Phone. This IP address of this machine will be tracked by the admin in our system and admin can delete such malicious user.

4. COLLUSION ATTACK

Whenever user gives the fake feedbacks about the product multiple times in order to either increase or decrease the productivity or ratings of products this type of attack is called as Collusion attack. This type of malicious behaviour can occur in a non-collusive way where a particular malicious user gives multiple misleading feedbacks to conduct a self-promoting attack or a slandering attack.

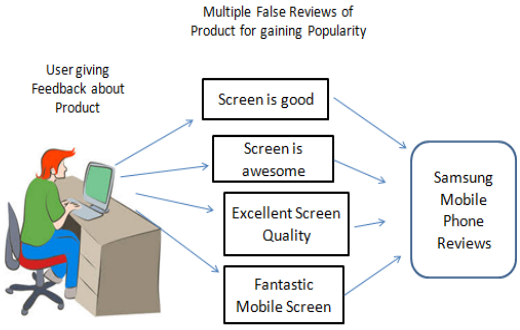

Fig -2: Collusion Attack

In this figure, single user given the multiple feedbacks about the Samsung Mobile Phone as "Screen is good", "Screen is awesome", "Excellent screen quality ", "Fantastic mobile screen" , but from the same user account. It means the user is just trying to increase the counts of reviews (which are fake).

Our system provides the facility to the admin to delete such type of malicious user in order to prevent the system.

5. CONCLUSION

In our system, we focused on detecting topical relations between opinion targets and opinion words. The Hierarchical Database Model that will gather the data and store it into the database in a hierarchical manner. Our system also covers the attacks like Collusion and Sybil attacks for defending system from malicious users. The future scope of this system is that it can also be applied to different Online Social Websites like Facebook, Twitter, etc which would become more beneficial and secure for the users.

ACKNOWLEDGEMENT

We are grateful to our guide Mr. S. N. Shelke for their encouragement and guidance. We would like to thank Head of Department Prof. Mr. B. B. Gite who has morally supported for the project. We also want to thanks to our Principal Dr. K. P. Patil Sir. He always supports us for different activities and guides us to achieve the success. At last but not least, we also thankful all the friends,

colleagues who gave us lot of support to successfully complete the project.

REFERENCES

[1] Talal H. Noor, Quan Z. Sheng, Lina Yao, Schahram Dustdar, Anne H.H. Ngu, "CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services," IEEE Transactions on Parallel and Distributed Systems, Vol. 27, No. 2, February 2016

[2] S. M. Khan and K. W. Hamlen, "Hatman: Intra-cloud trust management for Hadoop," in Proc. 5th Int. Conf. Cloud Comput., 2012, pp. 494–501.

[3] S. Pearson, "Privacy, security, and trust in cloud computing," in Privacy and Security for Cloud Computing, Ser. Computer Communications and Networks. New York, NY, USA: Springer, 2013, pp. 3–42.

[4] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," J. Cloud Comput., vol. 2, no. 1, pp. 1–14, 2013.

[5] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[6] E. Friedman, P. Resnick, and R. Sami, "Manipulation-resistant reputation systems," in Algorithmic Game Theory. New York, USA: Cambridge Univ. Press, 2007, pp. 677–697.

[7] J. R. Douceur, "The Sybil Attack," in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., 2002, pp. 251–260.

[8] S. Ba and P. Pavlou, "Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior," MIS Quart., vol. 26, no. 3, pp. 243–268, 2002.

[9] M. Shahira Banu, S. Lakshmi Narasimman, "A Survey On Sybil Attacks In Social Networks", International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 4, Issue 3, March 2015

[10] Urvashi Tripathy, Professor Shriram Yadav, "Centrally Organized Neighbor Similarity Trust against Sybil Attack in P2P E - Commerce", International Journal of Advanced Research in Computer Science and Software Engineering 6 (2), February - 2016, pp. 147 – 151.