INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 3 (2017) PAGES 2522 - 2526
RECEIVED : 27.05.2017 PUBLISHED : 22.06.2017
May 22, 2017

CLOUD SHIELD: ENHANCED ZKC2P USING MULTIPLE ATTACKS IN TRUST MANAGEMENT

[1]Yaminipriya R, [2]Dr.S.V.Sudha,
[1]PG Scholar, Department of Computer Science and Engineering, Professor and Head, Dr.N.G.P Institute of Technology, Coimbatore, India.
[2]Department of Computer Science and Engineering, Dr.N.G.P Institute of Technology, Coimbatore, India.

ABSTRACT

In any online e-commerce application reviews play a very important role. Large part of the customers read reviews of products or stores before making the decision of what or from where to buy and whether to buy or not. As writing fake reviews comes with monetary gain, there has been a huge increase in deceptive opinion spam on online review websites. Basically fake review or fraudulent review or opinion spam is an untruthful review. Positive reviews of a target object may attract more customers and increase sales as well as negative review of a target object may lead to lesser demand and decrease in sales. Both are comes under fake review category only. Traditional methods of data analysis have long been used to detect fake reviews. Early data analysis techniques were oriented toward extracting quantitative and statistical data characteristics. In order to overcome these problems in this paper we introduction multi model attacks to ensure the security to ensure the security. The multi attack model will work together to form a cloud shield for trust management. In the proposed system there are seven attacks are implemented to ensure the cloud armour. The attacks are follows: Collusion attack, Sybil attack, Cascade based attack, Time based Registration attack, Day based Registration attack, Text pattern attack (Positive) and Text pattern attack (Negative). An option generation will be created with the consideration for seven attacks and finally trustworthy will be generated.

Keywords: Multi Model Attack, Cloud Computing, Text pattern, fake reviews and trustworthy.

1. INTRODUCTION

Cloud computing refers to the underlying infrastructure for an emerging model of service provision that has the advantage of reducing cost by sharing computing and storage resources, combined with an on demand provisioning mechanism relying on a pay-per-use business model. These new features have a direct impact on information technology (IT) budgeting but also affect traditional security, trust and privacy mechanisms.[1] Trust is a critical factor in cloud computing; in present practice it depends largely on perception of reputation, and self assessment by providers of cloud services. We begin this paper with a survey of existing mechanisms for establishing trust, and comment on their limitations.[2]. Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized data centre resources, uphold user privacy, and preserve data integrity. The authors suggest using a trust-overlay network over multiple data centres to implement a reputation system for establishing trust between service providers and data owners.[3]. Cloud computing provides cost-efficient opportunities for enterprises by offering a variety of dynamic, scalable, and shared services. Usually, cloud providers provide

assurances by specifying technical and functional descriptions in Service Level Agreements (SLAs) for the services they offer [4]. Consumers' feedback is a good source to help assess overall trustworthiness of cloud services. However, it is not unusual that a trust management system experiences malicious behaviours from its users [5].

2. RELATED WORK

Customers are more dependent on making decisions to buy products either on ecommerce sites or offline retail stores. Since these reviews are game changers for success or failure in sales of a product, reviews are being manipulated for positive or negative opinions. Manipulated reviews can also be referred to as fake/fraudulent reviews or opinion spam or untruthful reviews. In today's digital world deceptive opinion spam has become a threat to both customers and companies. Distinguishing these fake reviews is an important and difficult task. These deceptive reviewers are often paid to write these reviews. As a result, it is a herculean task for an ordinary customer to differentiate fraudulent reviews from genuine ones, by looking at each review.

The adoption of cloud computing may move quite quickly depending on local requirements, business context and market specificities. The economic potential of cloud computing and its capacity to accelerate innovation are putting business and governments under increased pressure to adopt cloud computing based solutions.

ALGORITHM

PARTICLE SPAM FILTERING ALGORITHM

Initialization: Event e, session s → tuples, total comment Tc

< te start te end > and <ts start ;ts end; Es >

Generation: session s→Leading event Es

Extraction : Calculating 1:8 Ration for Positive boost and 8:1 for negative boost

If 1<=8 & 1*8 = >8 →Positive comment

If 8<=1 & 8*1=>1→ Negative comment

Evaluation: FD[0]arr; check up to >60, Fraudulent Range

PC >=5 FD[20]arr else 0, FD[0]arr

NC>=5 FD[20]arr else 0,FD[0]arr

Checking: FD[num]arr >60

PC >= 3 FD[20]arr if <3 FD[0]arr

NC>=3 FD[20]arr if<3 FD[0]arr

- Considering the posted comment from ANN will be initialized as PC as
- positive comment and NC as the negative comment.
- As per Opinion Mining 6 will be the least consideration and here the consideration will be 9 parameters.

- Buffer and Array will be FD[num]arr.
- As per commitment FD[>=60]arr will fraudulent user

3. METHODOLOGY

Users of decision support systems often see data in the form of data cubes. The cube is used to represent data along some measure of interest. Although called a "cube", it can be 2-dimensional, 3-dimensional, or higher-dimensional. Each dimension represents some attribute in the database and the cells in the data cube represent the measure of interest. For example, they could contain a count for the number of times that attribute combination occurs in the database, or the minimum, maximum, sum or average value of some attribute. Queries are performed on the cube to retrieve decision support information. In case a database that contains transaction information relating company sales of a part to a customer at a store location. The data cube formed from this database is a 3-dimensional representation, with each cell (p,c,s) of the cube representing a combination of values from part, customer and store-location. The contents of each cell are the count of the number of times that specific combination of values occurs together in the database. Cells that appear blank in fact have a value of zero. The cube can then be used to retrieve information within the database about, for example, which store should be given a certain part to sell in order to make the greatest sales. A data cube built from m attributes can be stored as an m-dimensional array. Each element of the array contains the measure value, such as count. The array itself can be represented as a 1-dimensional array. For example, a 2-dimensional array of size x x y can be stored as a 1-dimensional array of size x*y, where element (i,j) in the 2-D array is stored in location (y*i+j) in the 1-D array. The disadvantage of storing the cube directly as an array is that most data cubes are sparse, so the array will contain many empty elements (zero values). Rollup or summarization of the data cube can be done by traversing upwards through a concept hierarchy. A concept hierarchy maps a set of low level concepts to higher level, more general concepts. It can be used to summarize information in the data cube. As the values are combined, cardinalities shrink and the cube gets smaller. Generalizing can be thought of as computing some of the summary total cells that contain ANYs, and storing those in favour of the original cells.

4. ATTACK MODEL

- Collusion attack: Checks for basic count and checks the rank to eliminate the users.
- Sybil attack: It checks the unique IP address users. More repeated user's form same IP address will be verified here. The account creation IP address is more important.
- Cascade based attack: This works on the purchase method. Whether the user commenting the after the purchase or commenting without purchase.
- Time based Registration attack: It monitors for login and login methods. More comments from minimum login leads to elimination.
- Day based Registration attack: It checks for number of days. The opinion will generate for number login vs number of days
- Text pattern attack (Positive): Checks for positive comments
- Text pattern attack (Negative): Checks for negative comments

FUTURE ENHANCEMENT

Even the system is working well according to the commitment; still we need some enhancement to make the system more efficient and better. Being ecommerce application has been used in this application, as the content management system, the system need to meet out the latest technology. The ecommerce application will work efficiently on cloud computing, our current system will be supporting on cloud computing. Our future work will be based on the Green Computing. Green computing overcomes all the drawbacks in the cloud computing. Our system supports client server architecture also.

CONCLUSION

Detecting the fraudulent reviews and ensuring cloud armour has been developed. Initially the application environment is created with an admin. This ecommerce dataset has a product and review based communication between the seller and the user. Here the data training is done using the data dictionary in which the admin can update the positive and negative words. Based on this data training the text is categorized in to positive, negative and neutral comments. Here categorization is implemented for sentimental data analysis. These methods will analysis the input data from the data set. Each sentence will be analyzed with text categorization methods. So that positive words and negative words will be compared accordingly. The fake reviews are identified through analyzing various parameters such as numbers of repeated comments, number of comments for the same product and so on. Once the repeated comments are identified and it is removed from the comment list. Thus trust has been implemented

REFERENCE

[1] Trust Mechanisms for Cloud Computing. J. Huang and D.M.Nicol, “Trust Mechanisms for Cloud Computing,” Journal of Cloud Computing, vol.2,no.1,pp.1–14,2013

[2] Trusted Cloud Computing with Secure Resources and Data Colouring. K.Hwang and D.Li, “Trusted Cloud Computing with Secure Resources and Data Coloring,” IEEE Internet Computing, vol.14, no.5,pp.14–22,2010.

[3] Towards a Trust Management System for Cloud Computing. S.Habib, S.Ries, and M.Muhlhauser, “Towards a Trust Management System for Cloud Computing,” in Proc.of TrustCom’11, 2011

[4] Service-oriented Computing and Cloud Computing: Challenges and Opportunities. Y .W ei and M.B.Blake, “Service-oriented Computing and Cloud Computing: Challenges and Opportunities,” Internet Computing, IEEE, vol.14,no.6, pp.72–75,2010.

[5] A. Perrig, R. Szewczyk, W. Wen, D. Culler, and J. Tygar, “SPINS: Security protocols for sensor networks,” Wireless Networks Journal (WINET), vol. 8, no. 5, pp. 521–534, Sep. 2002.

[6] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, “Tinypk: securing sensor networks with public key technology,” in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN ’04). New York, NY, USA: ACM, 2004, pp. 59–64.

[7] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in Proceedings of the 7th international conference on Information processing in sensor networks (IPSN '08). IEEE Computer Society, 2008, pp. 245–256.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[21] J. L. X. Li, M. R. Lyu, "Taodv: A trusted aodv routing protocol for mobile ad hoc networks," in Proceedings of Aerospace Conference, 2004.

[9] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefs-tathiou, C. Vangelatos, and L. Besson, "Design and implementa-tion of a trust-aware routing protocol for large wsns," International Journal of Network Security & Its Applications (IJNSA), vol. 2, no. 3,Jul. 2010.

[10] A. Rezgui and M. Eltoweissy, "Tarp: A trust-aware routing protocol for sensor-actuator networks," in IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS 2007), 8-11 2007.

[11] S. Chang, S. Shieh, W. Lin, and C. Hsieh, "An efficient broadcast authentication scheme in wireless sensor networks," in Proceedings of the 2006 ACM Symposium on Information, computer and communications security (ASIACCS '06). New York, NY, USA: ACM, 2006, pp. 311–320.

[12] S. Ganeriwal, L. Balzano, and M. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sen. Netw., 2008.

[13] G. Zhan, W. Shi, and J. Deng, "Poster abstract: Sensortrust - a re-silient trust model for wsns," in Proceedings of the 7th International Conference on Embedded Networked Sensor Systems (SenSys'09), 2009.

[14] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis, "Collection tree protocol," in Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys '09). New York, NY, USA: ACM, 2009, pp. 1–14.

[15] S. M. Khan and K. W. Hamlen, "Hatman: Intra-Cloud Trust Management for Hadoop," in Proc. CLOUD'12, 2012.

[16] S. Pearson, "Privacy, Security and Trust in Cloud Computing," in Privacy and Security for Cloud Computing, ser. Computer Com- munications and Networks, 2013, pp. 3–42.

[17] J. Huang and D. M. Nicol, "Trust Mechanisms for Cloud Com- puting," Journal of Cloud Computing, vol. 2, no. 1, pp. 1–14, 2013.

[18] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14–22, 2010.