16-17

Volume 4, Issue 5, May-2017, pp. 161-168 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

IJCERT

Available online at: www.ijcert.org

Product Rating using Opinion Mining

[1]Sunil B. Mane, [2]Kruti Assar, [3]Priyanka Sawant, [4]Monika Shinde

[1] Assistant Professor, Department of Computer Engineering and Information Technology, College of Engineering Pune Pune - 411005, Maharashtra, India.

[2,3,4] B.Tech Student, Information Technology, College of Engineering Pune Pune - 411005, Maharashtra, India.

Abstract :- Amazon.com is one of the largest electronic commerce website in the world which allows users to purchase different products and submit reviews on each one of them. The reviews allow the first-time buyers to understand the quality of the products and decide whether to make a purchase or not. The reviews result in unstructured big data which can be analyzed and used for recommendation of a product on the website. However, it is possible that some customers write fake reviews to promote or defame a particular brand. So it is important to detect and remove the fake reviews for providing the correct rating to the product. Also, it is necessary to create a fast and efficient system for analyzing big data. The present systems used for big data analysis are quite slow. So here, we use the Apache Spark framework for increasing the speed of processing the Amazon reviews. This paper provides a new implementation for analyzing Amazon reviews which involve detection of fake reviews, processing the genuine reviews using Apache Spark and finally rating the products.

Keywords: Opinion Mining, Apache Spark, Product Rating, Fake Review Detection, Natural Language Processing, Sentiment Analysis.

1. Introduction

Over the years, with advancement in technology, the business strategy has also changed. Now many e-commerce websites have emerged which are adopting new innovative ideas for publicity. One of the most important marketing schemes is providing a platform for online customer reviews. These online reviews help the customer to analyze different products and services and also provide a platform for comparing prices before taking a decision. Moreover, companies and vendors can frame new business strategies depending on the opinions provided by customers.

Amazon encourages its customers to give their feedback and write reviews on its website which are then analyzed and the one with most "helpful" hits is displayed on the front page. However, what if these reviews are fake? Few cases have been identified where people post incorrect reviews to defame a brand, or sometimes exquisite reviews are posted to increase the sales of a product. Hence it is important to detect certain opinions and eliminate the rest.

The real reviews can further be classified into positive and negative opinions, and sentiment analysis is performed on this data to finally rate different products to help the customer select one out of them.

2. Literature review

Much research has been carried out on Opinion Mining which is explained below.

2.1 Fake Review Detection

Presently, Amazon website uses some machine learning algorithms to select relevant features and decide the
Final rating of a product. However, it does not apply any algorithm to detect whether a review is fake or not. Few websites like Yelp.com and Fakespot.com can be used to detect fake reviews online, but there is no particular algorithm known to the world to filter reviews. Only a few relevant rules are designed for

International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319 – 6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 4; April 2017; Page No. 3342-3345
DOI: http://dx.doi.org/10.24327/ijcar.2017.3345.0267

Research Article

AUTHENTIC TECHNIQUES OF AUTHENTICATION IN MICROSERVICES

Shagufta N. Shaikh[1] and Sunil B. Mane[2]

[1]Department of Computer Engineering, College of Engineering Pune, Pune – 411005
[2]Department of Computer Engineering & IT, College of Engineering Pune, Pune – 411005

ARTICLE INFO

Article History:

Received 19th January, 2017
Received in revised form 10th February, 2017
Accepted 22nd March, 2017
Published online 28th April, 2017

Key words:

Microservices, OAuth 2.0, OpenID Connect

ABSTRACT

Microservices is the catch word of the town nowadays. The microservices are small, autonomous services doing a single task, and performing it well. However various concerns such as security in microservices are not explored yet. This paper presents a comparison of the existing protocols such as 2-way SSL, HMAC, SAML, etc. used for authentication and authorization of the end users by the service providers. It also explores the concerns where they lack and presents a model implementing OpenID Connect. It presents a proper comparison to propose OpenID Connect to be best of the lot.

INTRODUCTION

The rudimentary approach for developing software has been the monolithic way. Monolithic approach is still good for small scale teams and projects, nevertheless once scalability, flexibility and other requirements like fast development, short time to market, wider team alliance, and so on becomes gradually critical to accomplish business competitiveness, monolithic halts being profitable. This is where the Microservices architecture comes to rescue. Microservices is responsible for an intensive, scoped and modular tactic for application design. Microservices are small, autonomous services that work together. [1] It can be well elaborated using keywords: 'Faster development and Speed to production'. Microservices are deceptively termed to be code of limited length. Conversely, microservices are a piece of code which performs a single task and performs it soundly. They are independent in failure i.e. failure of a single component does not force the entire system to breakdown at once. The term micro indicates the services to be lightweight and which cannot be further divided into sub tasks and performs one task solely with minimal dependency on other services. They are independently scalable as well. The most perplexing part of microservices is defining the granularity of the services.

Security in microservices is one of the least explored topics. This paper explores the various vulnerabilities in security and also presents the various methods deployed for providing authentication and authorization in microservices. Since microservices depends on the idea of loose coupling and high cohesion. They do not share any databases. If at all there are any dependencies among the microservices they use light weight communication mediums to achieve it. The most common and widely used communication methodology today are the REST APIs. REST APIs are simple, stateless and lightweight protocol used for communication. As REST: Representational State Transfer is stateless several traditional authentication and authorization techniques fail to suffice the purpose. Several protocols are being modulated for securing the REST APIs. However there isn't a standard protocol for securing microservices. This paper provides a crisp comparison of the several traditional and upcoming techniques for providing authentication as well as authorization in microservices. It also implements a model on the OAuth 2.0 and OpenID Connect techniques employed for the authentication and authorization in microservices.

The further sections of the paper is as follows: Section 2 briefs about the topics that gave motivation for this paper. Section 3 explains the various perspectives involved related to security in microservices. Section 4 describes the various traditional proposed solution for authentication and authorization in microservices. Section 5 presents the implemented model of the paper presenting OAuth2.0 and OpenID Connect techniques. Section 6 provides a crisp comparison of the strengths and flaws of the developed techniques. Section 7 puts forth the accomplishments of the paper.

LITERATURE SURVEY

Microservices has become a hot topic in field of software development. Its efficiency is well demonstrated by big giants like: Amazon, Netflix, eBay, etc. The book [1] on

Corresponding author:* **Shagufta N. Shaikh
Department of Computer Engineering, College of Engineering Pune, Pune – 411005