DISCOVERING TRAFFIC BOTTLENECKS HE DEVICES BY USING SERVICES

A

Seminar Report submitted to Savitribai Phule Pune University,Ganeshkhind

In partial Fulfillment for the awards of Degree of Engineering in Information Technology

Submitted by

Rohit B80418503

Under the Guidance of

Prof. R. U. Pawar

April, 2014- 15

Department of Information Technology

SNJB'S Late Sau. Kanatabai Bhavarlalji Jain,
College of Engineering, Chandwad
Dist:Nashik

SNJB'S Late Sau. Kanatabai Bhavarlalji Jain, College of Engineering, Chandwad Dist:Nashik

Department of Information Technology

2014-15

Certificate

This is to certify that the Seminar Report entitled *Discovering Traffic Bottlenecks he devices by using Services* submitted by Mr./Ms. **Rohit Pawar** is a record of bonafied work carried out at SNJB's K. B. Jain College of Engineering during academic year 2014-15,which affiliated to the Savitribai Phule Pune University.

Date:
Place: Chandwad

Seminar Guide
Prof. R. U. Pawar

Prof. P. R. Bhaladhare	**Prof. J. J. Chopade,**
HOD	**(I/C)Principal**
Department of Information Technology	

Examiner:..

Acknowledgement

I would like to acknowledge all the people who have been of the help and assisted me throughout my project work. First of all I would like to thank my respected guide Prof. R. U. Pawar, Professor in Department of Information Technology for introducing me throughout features needed. The time-to-time guidance, encouragement, and valuable suggestions received from him are unforgettable in my life. This work would not have been possible without the enthusiastic response, insight, and new ideas from her.

I am also grateful to all the faculty members of SNJB's College of Engineering for their support and cooperation.

I would like to thank my lovely parents for time-to-time support and encouragement and valuable suggestions, and thank my friends for their valuable support and encouragement.

The acknowledgement would be incomplete without mention of the blessing of the Almighty, which helped me in keeping high moral during most difficult period.

Rohit Pawar

Abstract

Searching for applications that are highly relevant to development tasks is challenging because the high-level intent reflected in the descriptions of these tasks doesn't usually match the low-level implementation details of applications . To reduce this mismatch we see an approach called EXEcutable exaMPLes ARchive (Exemplar) for finding highly relevant software projects from large archives of applications. Exemplar takes natural-language query that contains high-level concepts (e.g. MIME, data sets) as input, then uses information retrieval and program analysis techniques to retrieve applications that implement these concepts. For getting highly relevant application Exemplar ranks applications in three ways. First, consider the descriptions of applications. Second, examine the Application Programming Interface (API) calls used by applications. Third, analyze the dataflow among those API calls. Mainly Ranking mechanism also works in three ways 1) A component that computes a score based on word occurrences in project descriptions (WOS) , 2) A component that computes a score based on the relevant API calls (RAS) and 3) A component that computes a score based on dataflow connections between these calls (DCS) . The total ranking score is the weighted sum of these three ranking scores.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Need

1.2 Basic Concept

1.3 Application

1.4 Organization of the Report

Chapter 2

Literature Survey

The purpose of the literature survey is to identify information relevant to project work and the potential known impacts of it within the project area .This section should include a comprehensive report of current market survey done with respect to problem. Include study of similar systems available, if any along with their pros and cons. Identify those area where there is an absence or scarcity [2].

2.1 Other Technologies available to cater the same concept

2.2 Their advantages, disadvantages and limitations

Chapter 3

Details of analytic work

1. What is to be developed?

2. Technology Used

3. Parameters

[3]

Chapter 4

Details of Experimental work

Chapter 5

Conclusion

Conclusion should write in points, Point should be in simple language.

Bibliography

[1] T.-M. Koo, H.-C. Chang, and G.-Q. Wei, "Construction p2p firewall http-botnet defense mechanism," in *IEEE International Conference on Computer Science and Automation Engineering*, vol. 1, Aug 2011, pp. 33–39.

[2] H. Choi, H. Lee, H. Lee, and H. Kim, "Botnet detection by monitoring group activities in dns traffic," in *7th IEEE International Conference on Computer and Information Technology*, 2007, pp. 715–720.

[3] H. Choi, H. Lee, and H. Kim, "Botgad: detecting botnets by capturing group activities in network traffic," in *Proceedings of the Fourth International ICST Conference on Communication System Software and Middleware*, oct 2009, pp. 1–8.

[4] Govil and G.Jivika, "Criminology of botnets and their detection and defense methods," in *IEEE International Conference on Electro-Information Technology*, sept 2007, pp. 215–220.

[5] C. A, J. Binkley, and D. Harley, *Botnets: THE KILLER WEB APP.* SYNGRESS, 2007.

[6] M. T. Banday, J. A. Qadri, and N. A. Shah, "Study of botnets and their threats to internet security," *Sprouts: Working Papers on Information Systems*, pp. 9–24, 2009. [Online]. Available: http://sprouts.aisnet.org/9-24

[7] P. Wang, L. Wu, B. Aslam, and C. Zou, "A systematic study on peer-to-peer botnets," in *Proceedings of 18th IEEE International Conference on Computer Communications and Networks*, Aug 2009, pp. 1–8.

[8] G. Gu, J. Zhang, and W. Lee, "Botsniffer:detecting botnet command and control channels in network traffic," in *Proceedings of the 15th Annual Network and Distributed System Security Symposium*, February 2008.

[9] J. Nazario, "Blackenergy ddos bot analysis," *Arbor Networks*, oct 2007.

[10] N. Provos and T. Holz, *Virtual honeypots: from botnet tracking to intrusion detection.* Addison-Wesley Professional, 2007.

[11] Rohit, Pawar, and Holz, *SNJB from botnet tracking to intrusion detection.* Addison-Wesley Professional, 2007.