International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 08 | Aug 2019 www.irjet.net p-ISSN: 2395-0072

Windows Log Investigator System for Faster Root Cause Detection of a Defect

Mr. Akshay Wankhade[1], Prof. Pramila M. Chawan[2]

[1]M.Tech Student, Dept. of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India
[2]Associate Professor, Dept. of Computer Engineering and IT, VJTI College, Mumbai, Maharashtra, India

---

Abstract – *It is my attempt to make a log analysis system for developers to help them in solving the problems, and to provide assistance for an interactive Log System analysis experience. The incentive behind this effort is to significantly reduce the difficulties faced by developers while solving a defect. To reduce said difficulties, we designed a log analysis algorithm to solve the difficulties faced by developers, which is developed with help of C# and the WPF architecture. The user has a provision to take a log analysis report. The method of testing we have used is the backtracking algorithms for testing. The algorithm will allow us to determine which type of defect is occurred and what will be the possible solution for it. This log analysis System is not only limited to Developers, but also to persons who are using the particular application.*

Key Words: Log Analysis, C# Technology, WPF Architecture, Backtracking Algorithm.

1. INTRODUCTION

Log Investigator is the place where transactions are carried out with the help of the Windows log investigator. Log investigator have an interactive graphical user interface so normal people can see the results easily. Problem occurs when any application get crashed due to n reasons to solve that problem we have provided a more efficient way to generalized the different events that are captured by the windows events log. Perhaps this problem can be mitigated. Problem identification is the main aspect, which is responsible for the recognition of items and the satisfaction of the problem solving.

Previously the Defects are Manage and solve by the experienced developers. It was a very challenging situation for Managers to continuously hire developers with experience and having the capability of solving the defect. Due to which few machine-learning techniques were introduced in order to process large amounts of data without failing. Pattern Recognition techniques have gained popularity over the years because of their ability in discovering practical knowledge from the database and transforming them into useful information. Accuracy of prediction for each of these available techniques varies according to the methods used and the scenario or which it is built.

Presently, a lot of research has been done to develop models based on artificial neural networks. Many different training techniques have been incorporated and have shown to improve accuracy. Currently the defect is assigned a life cycle, also known as Bug Life cycle is the journey of a defect cycle, which a defect goes through during its lifetime. It varies from organization to organization and from project to project as it is governed by the software testing process and depends upon the tools used. Once the tester posts the bug, the lead of the tester approves the bug and assigns the bug to developer team. There can be two scenarios, first that the defect can directly assign to the developer, who owns the functionality of the defect. Second, it can also be assigned to the Dev Lead and once it is approved with the Dev Lead, he or she can further move the defect to the developer. In India, currently, company use traditional way to solve a bug based on severity of bug that already been trained. Little work is done to improve the accuracy of solving the defects.

1.1 LITERATURE REVIEW

One way event logs can be helpful during an investigation is to search for certain artifacts that will help identify the source of an attack. The IP address is an important key when trying to locate a specific individual or group. This is one of the reasons various event logs are so important for the collaboration and confirmation of other hard data found on the system or network. IP Addresses by themselves cannot be filtered using the event log as the filtering mechanism. However, a specific IP can be found by using Microsoft's Power Shell Get NetIPAddress Cmdlet (Microsoft, 2012). Another way to get IP addresses would be to create a custom view and use the XML tab to write the query (Paper Cut, 2013). One case where IP addresses were a key point in the investigation is the APT1 unit Cyber Espionage attack. Mandiant, one of the leading security companies, released a report concerning one of the Cyber Espionage units in China (Mandiant, 2013). Mandiant named the unit "APT1". 8 An Advanced Persistent Threat (APT) has become the most common attack on enterprise level network systems. Well-funded and educated Nation States such as China or other criminal groups conducting cyber espionage (Cloppert, 2009) usually carry out APT attacks. Mandiant responded to 150 victims in seven years that APT1 had stolen vast amounts of data from application.

In this paper, author discussed decision-tree-based SVM and the separability measure between lasses based on the distribution of the classes. To improve the generalization ability of SVM decision tree, a novel

separability measure is given based on the distribution of the training samples in the feature space. Based on the idea that the most easily separated classes are separated firstly during the decision tree is formed, and by introducing the defined separability measure in feature space into the formation of the decision tree, an improved algorithm for decision-tree-based SVM is obtained. Classification experiments for different data sets prove the performance improvement of the improved algorithm for decision-tree- based SVM.

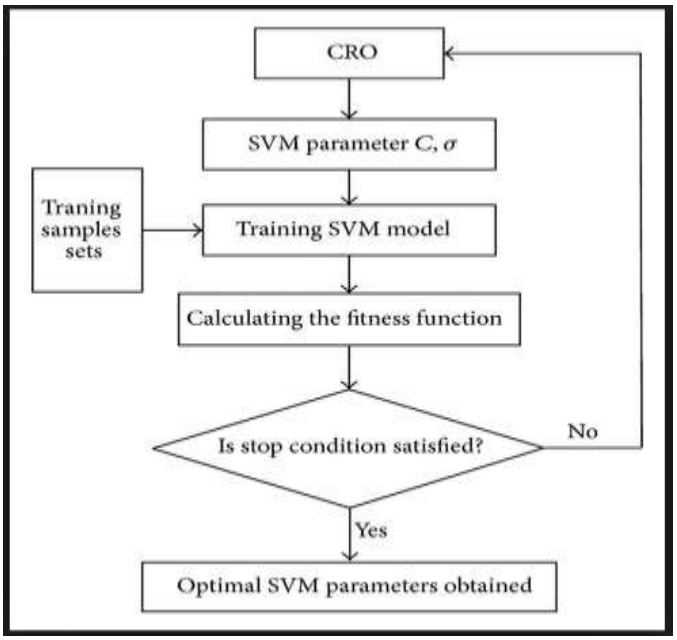

Figure 1 : SVM

On Weighting Clustering, this paper is the first attempt at its formalization. More precisely, we handle clustering as a constrained minimization of a Bregman divergence. Weight modifications rely on the local variations of the expected complete log-likelihoods. Theoretical results show benefits resembling those of boosting algorithms and bring modified (weighted) versions of clustering algorithms such as k-means, fuzzy c-means, Expectation Maximization (EM), and k-harmonic means. Experiments are provided for all these algorithms, with a readily available code. They display the advantages that subtle data reweighting may bring to clustering. The main contribution of this paper is to adopt an insight from classification to improve the performance of unsupervised learning algorithms by making more precise this analogy to boosting algorithms. The raw data is extracted by meter, which install on the main electric entrance of the resident, the mean-shift clustering is based on the data after events detector processing, and the result of clustering is used as input data of final identification.

An actual residential trail is given to show the clustering is available in the NILM system.

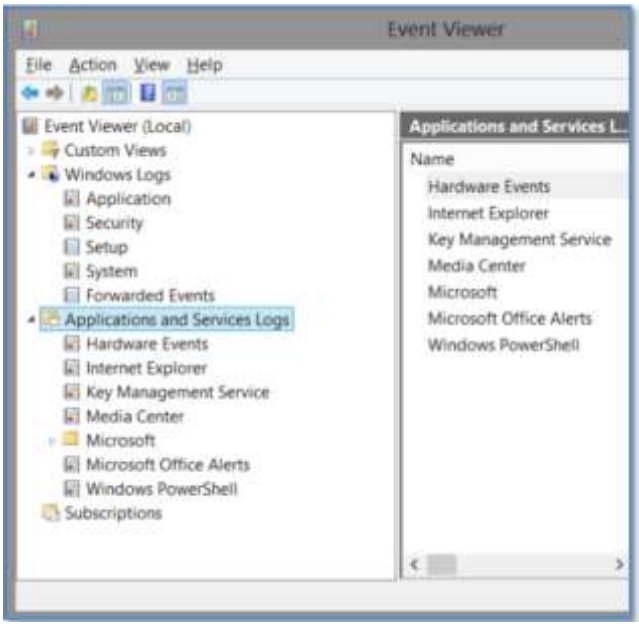

Figure 2 : Event Viewer

One way event logs can be helpful during an investigation is to search for certain artifacts that will help identify the source of an attack. The IP address is an important key when trying to locate a specific individual or group. This is one of the reasons various event logs are so important for the collaboration and confirmation of other hard data found on the system or network. IP Addresses by themselves cannot be filtered using the event log as the filtering mechanism. However, a specific IP can be found by using Microsoft's Power Shell Get NetIPAddress Cmdlet (Microsoft, 2012). Another way to get IP addresses would be to create a custom view and use the XML tab to write the query (Paper Cut, 2013). One case where IP addresses were a key point in the investigation is the APT1 unit Cyber Espionage attack. Mandiant, one of the leading security companies, released a report concerning one of the Cyber Espionage units in China (Mandiant, 2013). Mandiant named the unit "APT1". 8 An Advanced Persistent Threat (APT) has become the most common attack on enterprise level network systems. Well-funded and educated Nation States such as China or other criminal groups conducting cyber espionage (Cloppert, 2009) usually carry out APT attacks. Mandiant responded to 150 victims in seven years that APT1 had stolen vast amounts of data from application.

2. IMPLEMENTATION

Design and coding our Log Investigator Tool will be done through Microsoft Visual Studio Software, which provide all required libraries and simple API for making a Windows Application. We will built and design the Windows pages and

graphical user interface in C# language, since it is a lightweight language, and works significantly faster in any given network. In addition, the user interface made from WPF architecture is 'responsive'; that is to say, it can adjust its scaling dynamically according to your screen resolution. Different effects can be applied to the Tool like, for instance: auto scrolling, Pattern Recognition, Automatic Data Storage Sensor when mouse over event is detected. The application itself is having the ability to store the data with different

Figure -1: Flow of Log Investigator System

I propose to improve the pattern recognition techniques by storing the randomized pattern and the root path of the defect which mostly similar in many defects. Methods are effective such as graph plotting for implementation and Boosted graph plots are much more effective than normal event viewer is. In my modified algorithm, clustering of the training dataset is done before plotting on graph.

In addition, we have designed a test module, which contains Log analysis test, which gives diagnosis based on the result. The two-color curve to be used in the graph-plotting test were pre-categorized depending on the different diagnosis possible. This simplifies the algorithm to determine the type of the defect, which is causing the problems to crash, or misbehaving nature of the application due possible numbers of reasons it can run time exceptions or any functionality, which is causing the data to change the behavior rather than expected behavior.

The flow of the application is similar to linear approach the application will get the input file as .evtx file which is a log file generated by the windows event viewer application. After providing input to the application, the application will store the data into particular structured format to get the analysis done by the developers. The calculations and everything will be done inside the filtering section as shown below.

Figure -2: Filtering Requirements Configuration File

In Requirement filtering the windows configuration is filtered with the System 1 requirements so that it can check whether the application is meeting the minimum software requirements or not. It is found that many times whenever any defect occurs developers try to directly solve the problem. Rather than checking, the requirements and later on it may found that the application was not meeting the software requirements. Due to which user end up taking too much time for solving the problem which not even a valid defect. So to avoid this type of situations we have developed a more sophisticated and user friendly tool which will match the minimum requirements with valid requirements based on that it will provide the results if application shows any red color that means it is not meeting the requirements if everything is green then developer has to look for the errors.

2.1 RESULT

Figure -3: Result after Loading the Events

Here we diagnosed the defect type with our module by using graph-plotting test. Previously the Defects are Manage and solve by the experienced developers. It was a very challenging situation for Managers to continuously hire developers with experience and having the capability of solving the defect. Pattern Recognition techniques have gained popularity over the years because of their ability in discovering practical knowledge from the database and transforming them into useful information. Depending on what method is used to learn the policy and how the training is carried out, the model will produce results.

Figure -4: Reduced Events with Time Slider

Now the Above figure shows that the application is changing the events in the time slider. That time slider is divided with the events with respect to time and occurrence of the application-crashed data. It helps the developers to identify the application defect root cause with respect to time and space configuration of application. This will reduce the time to look into all the events, which do not require for a specific time. Instead of that the developer can set the timeline to particular period and will focus on the most important part of the events this will reduce the developers time to identify the root cause of the defect. Similarly, the application has the ability to expand the events with respect to timeline by adjusting the range slider.

Figure -5: Increased Events with Time Slider

3. FUTURE SCOPE

Our future scope involves expanding the operation and quality to accommodate a larger customer base. It would mean scaling the database and upgrading the respective servers. Another feature to explore would be a smart personal assistant; it would identity patterns in the user's interests using machine learning and artificial intelligence. This would be a cornerstone is smart suggestion to the user; suggestions of style and apparels.

Another future objective intent is to expand to the smart-phone platform. We have plans to expand the System 1 portal into the Android and iOS platforms. Data sharing and interoperability between these platforms is required to have sync between the carts the user wishes to maintain across the various devices at his disposal, but within his account. This data-interchange can be implemented using JSON.

The enhancement feature for Root Cause Detection of defect by users must not be limited to developers, but rather must expand to other applications as well; to bring confidence to the Developers, and bring to them what they could not reach before.

4. CONCLUSIONS

This paper introduces a new way of solving the defect of application by users. Therefore, they can go and check whether they have one of the mentioned conditions, with the help of the graph-plotting test. After the testing is done, they are provided with a results of diminished patterns and enhanced results as per their diagnosed condition. Thus, here, we have improvised and modified the developer experience and reduce the trials faced by user individuals. In addition, we use a flat and responsive graphical user interface for this web application, which requires a lot less time and data to load over the Internet. Furthermore, this website is highly interactive and responsive as to even dynamically scale itself to the user's screen resolution. By adding such aforementioned extra features in our Windows application, we try to overcome the flaws of any generic application regarding all the users.

As we understand from the literature survey, there are many algorithms are available for pattern recognition, however there is lot of manual work involved in creating the data set for building log investigator using these algorithms. Since there is a scarcity of data, the model trained is not suitable for real world task. In addition, some drawbacks, which include proper prediction of the defect, are solved by using event viewer. To device a robust policy, the model needs to be trained rigorously with the help of Machine learning. The algorithm will be able to effectively predict the Root cause of defect based on previous data. It will be able to estimate the severity level that should be granted to a developer if it is customized. I stress on building a general algorithm in order to estimate its accuracy and its improvement over other available techniques. This algorithm will be trained on available datasets and tested on the same. Companies will be able to customize it as per their requirements.

REFERENCES

[1] Bhagya R Navada, Santhosh K, Prajwal S, Harikishan B Shetty, “An Image Processing Technique for Color Detection and Distinguish Patterns with Similar Color: An aid for Color Blind People,” Proceedings of International Conference on Circuits, Communication, Control and Computing (I4C 2014).

[2] Orazio Gambino1, Ester Minafo, Roberto Pirrone & Edoardo Ardizzone, “A Tunable Digital Ishihara Plate for Pre-School Aged Children,” Proceedings of International Conference on Circuits, Communication, Control and Computing (I4C 2014).

[3] About the XAMPP project, https://www.apachefriends.org/about.html

[4] Hideaki Orii, Hideaki Kawano, Hiroshi Maeda and Takaharu Kouda,, "Color Conversion Algorithm for Color Blindness using Self-Organizing Map," 978-1-4799-5955-6/14©2014 IEEE.

[5] S Poret, R D Dony, S Gregori, "Image Processing for Colour Blindness Correction," 978-1-4244-3878-5/09©2009 IEEE.

[6] Ingeborg Schmidt, "Effect of Illumination in Testing Color Vision with Pseudo-Isochromatic Plates," Journal of the optical society of America volume 42,number 12 December 1952.

[7] Rodney d. steinmetz, m.d., and Thomas p. kearns , m.d., "H-R-R PSEUDO-ISOCHROMATIC PLATES*," Section of Ophthalmology, Mayo Clinic, and the Mayo Foundation. The Mayo Foundation is a part of the Graduate School of the University of Minnesota.

[8] http://www.eyequant.com/blog/2013/07/02/108-million-web-users-are-color-blind-how-do-they-see-your-website.

BIOGRAPHIES

Mr. Akshay A. Wankhade
Mtech Student, Dept. Of Computer Engineering and IT,VJTI College, Mumbai, Maharashtra, India

Prof. Pramila M. Chawan
Associate Prof, Dept. Of Computer Engineering and IT,VJTI College, Mumbai, Maharashtra, India