Network Fault Root Cause Analysis (RCA) Using Supervised Machine Learning Approach

Zewdu Minyhun
HiLCoE, Computer Science Programme, Ethiopia
zwithgod@gmail.com

Dereje Teferi
HiLCoE, Ethiopia
School of Information Science, Addis Ababa University, Ethiopia
dereje.teferi@gmail.com

Abstract

Root Cause Analysis (RCA) is a daily and routine task performed by most telecom operators of multi-domain and multi-vendor heterogeneous networks. It is done mainly to minimize Service Interruption Time (SIT) and restore service as rapidly as possible. Existing RCA investigation techniques are still inaccurate, time consuming, manual and often carried out with the aid of domain experts who manually analyse and associate various technologies' data; namely, transmission, power, IP, mobile core, mobile access and fixed access domains in order to come up with the most probable cause of the problem. One solution to such problems is enabling machines to perform this task and automating the whole RCA task. Compared to the current investigation technique, this solution is faster due to automation of the entire RCA process. The solution is also cost effective because it needs fewer or no personnel to operate.

This paper provides a comparative analysis of RCA using different supervised machine learning algorithms called classifiers. Classifiers utilize training data to understand how a given incident relates to the cause, which is something that existing network fault management systems fail to do. It also shows that self-machine learning (learning from data without being programmed) approach is a promising solution to RCA by comparing the proposed approach with the traditional RCA approaches and previously conducted research works.

Keywords: Root Cause Analysis; Machine Learning; Multi-domain; Heterogeneous Networks

1. Introduction

Knowing the root cause enables telecom operators to quickly focus on problems affecting the service and provides the capability to troubleshoot and immediately resolve problems within a short period of time. We are primarily motivated by the following two challenges:

i. Traditional RCA Investigation Methods

Even though efforts have been made to automate and control alarm floods for many years, telecom operators in various countries are still using rule-based systems with trial and error investigation method. One of the techniques used is rule based system. Rule-based systems do not require profound understanding of the underlying network architecture and working principles and, for small networks, can be used as tools for fault diagnosis and root cause analysis [1]. However, as a network becomes larger and heterogeneous, new challenges arise, such as:

- Most paradigms for RCA, including rule-based systems, association-based reasoning, logic-based reasoning, cause and effect based reasoning, are configured out-of-the-box (i.e., predefined) and most of them need intervention by domain experts for corrective action and they don't learn from past experiences. Therefore, they do not respond properly to new situations.
- "*Maintaining Users-in-the-Loop (UIL)",* i.e., telecom operators usually make equipment, software, and network changes or modifications of existing systems and programs in order to accommodate new customer requests. As new changes are made to the network or old ones are updated, the characteristics of the alarms as well as the RCA rule need also change. Therefore, to evolve with the network, operators are required to understand the business rule,

modify the RCA rule and maintain end users informed, which is demanding, time consuming and painstaking.

- *Demand for reliable service:* telecom operators are in the strongest competition than ever before, as this sector gets new competitors. Hence, providing reliable services to maximum customer satisfaction will be one of the most crucial competitive advantages. This needs automated RCA systems for timely fault isolation and diagnosis and fulfilling SLAs (Service Level Agreements) within the agreed time frame. The question will be how to deliver reliable service using traditional RCA investigation techniques.

ii. Large amount of alarm data

Heterogeneous telecom infrastructure consists of a number of interconnected networks such as transmission network with IP network, IP network with access network, transmission network with mobile network, and so on. Each network in turn contains several sub-networks and devices, and failure on one of these devices affects neighbouring devices, which in turn affect their neighbours and so on. For example, a power equipment failure in a given base station causes broadband and voice to be interrupted. Each affected network device triggers alarm messages alerting network operators about the malfunction, often flooding the fault management system with a huge number of alarms, making it difficult for the operator to process them and take corrective actions on time. Alarm flooding is a persistent problem in telecommunications [2]. It occurs when the number of alarms is much higher than can be effectively managed, and most of these alarms are redundant and false alarms, i.e., alarms that alert abnormal situation when there is none. To cope with alarm floods, operators employ several techniques such as alarm correlation [2, 3], rule-based alarm reduction [4], alarm filtering, alarm masking, alarm shelving, alarm grouping and alarm prioritization. However, all these techniques have limited capability in identifying the root cause and solving operator's problems. Many telecom operators and domain experts agree that the current RCA and fault isolation steps shown in Figure 1 are time-consuming, inaccurate, inefficient and often carried out with the help of domain experts.

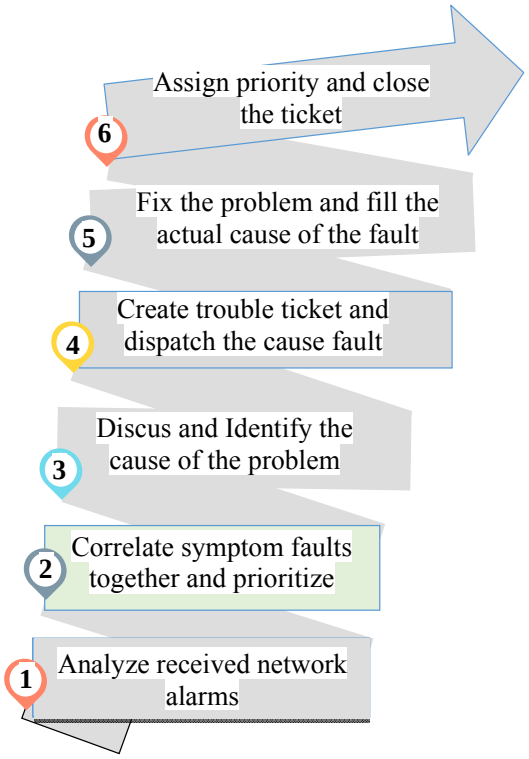


Figure 1: RCA Investigation Steps

To address these challenges, many operators and researchers conducted various studies using different techniques such as relational database [5], rule-based classification [6, 7], decision trees [6, 7], linear regression, logistic regression, cluster based [8], discriminant analysis, neural networks [7], and Naïve Bayes classification [6, 7]. However, all these studies are no longer viable for multi-domain and multi-vendor heterogeneous networks. Therefore, in this paper an investigation is undertaken using machine learning approach to isolate the primary cause (RCA) from a set of interrelated faults using different fault classification algorithms and techniques as a solution for a robust service assurance and end-to-end fault management.

2. Related Work

Using data mining and machine learning, several researches on a homogenous network have been made on RCA as a result of the technical developments in the field, advancement in data analytics research, availability of data, and increased

computing power. This section discusses some of the most related researches performed on RCA.

A hybrid approach to classify power system fault has been proposed by Babu and Mohan [17]. The proposed technique uses multiple SVM models with features extracted using Empirical Mode Decomposition and Hilbert Huang Transform algorithms. To realize their proposal, the authors used five major stages: data acquisition, pre-processing, feature extraction, feature selection and classification. Classification is done among ten fault cases with rigorous training and testing phases. The training set consists of two attributes and a target value called class label (usually -1 or 1). In each testing phase, SVM classifies the fault as class -1 if the fault is detected in corresponding phase and class 1 if not detected. Finally, the authors demonstrated the feasibility of their methodology using simple power system network. SVM performs well especially when feature areas of the domain are known in advance and when there are smaller number of instances. However, according to recent literature [18], this methodology is less efficient especially when large datasets are used and makes it less applicable for proactive monitoring and time sensitive applications.

Attempts were also made by Rozaki [6] using rule-based data mining classifiers to classify mobile network faults. The author extracted frequently embedded sub trees using decision tree algorithm and associated them with known class of the network fault under consideration. Then the author used structural rules for prediction and to determine the likelihood for a fault to come under a particular class and the outcomes of are satisfactory. In addition to this, the author also proposed a systematic approach for anomaly detection based on KPI data analysis modelling using Weka environment to monitor and optimize GSM network. The overall result showed that the proposed approach is capable of classifying Mobile faults with better accuracy than J48 and Bayesian network.

Molinero [10] also proposed Bayesian based RCA model for trouble ticket analysis. To build Bayesian model, the author used different trouble attributes such as type of element, symptoms, severity, area, affected service, etc., and generated a model called 'Bayesian network tree', and applied to new tickets to predict whether they have a root cause or not. A problem of Bayesian approach is that it does not take into consideration the interactions between different variables and, applying them on applications where there is a strong association among variables can lead to incorrect predictions.

Felldin [9], using Ericson's mobile network, showed the feasibility of using machine learning as an alternative solution to replace or aid humans on fault classification and root cause analysis. Rozaki [7] and Gosavi [11] also indicated the chosen method has been successfully applied to problems of similar nature with positive results.

Even if many of the key concepts remain the same (including goals and techniques), to the best of our knowledge, there is no research work done on multi-technology and heterogeneous network.

3. The Proposed Solution

A major problem of most root cause analysis systems is lack of ability to learn from data/examples or adapt to situations that are not hard-coded. Therefore, this section discusses the implementation aspect of a self-learning RCA system that automatically learns from known rules and archived fault data. Components of the proposed solution are shown in Figure 2 and each is described below.

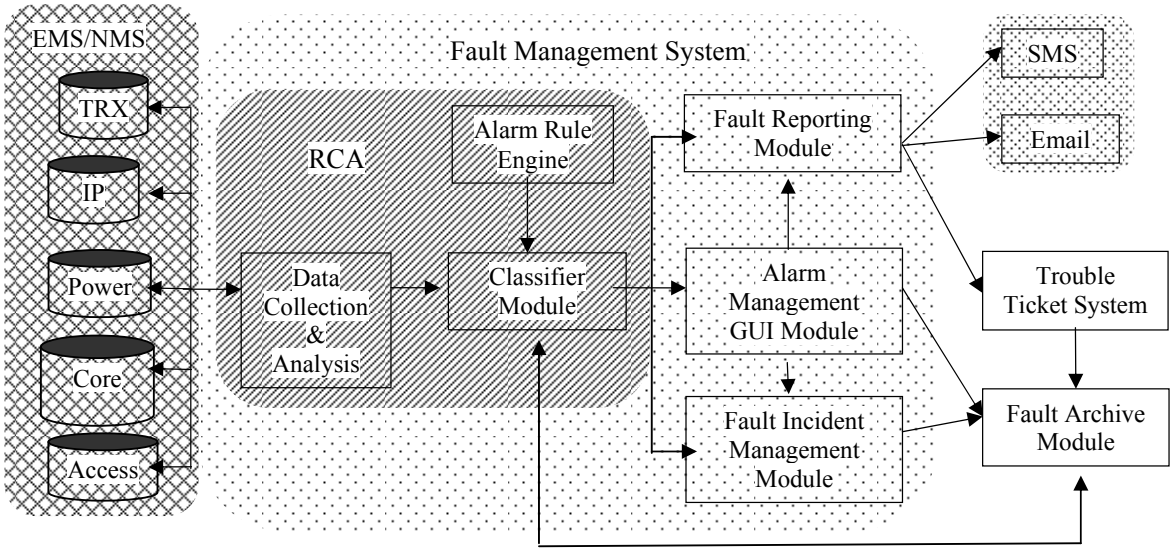


Figure 2: The Proposed Self-learning RCA Architecture

a. *Data Collection and Analysis Module:* collects real-time alarms from different network equipment and processes.

b. *Alarm Rule Engine:* generates rules for root cause analysis by considering the impact of each fault type on the network. Its main purpose is to define known business rules as input for the learning process.

c. *Classifier Module:* adopts distributed architecture combined with advanced rule engine and machine leaning technology, realizes RCA engine, and identifies cause alarms efficiently and effectively. It builds the classification models based on feedback obtained from the alarm rule engine and off-line training data.

d. *Alarm Management GUI Module:* is a web-based GUI for monitoring and analysing received alarms. It provides different functionalities on alarms such as acknowledge, filter, comment, clear, etc.

e. *Fault Incident Management Module:* notifies incidents to incident management units, operation and maintenance team, and other concerned personnel via email, SMS, alerts, etc.

f. *Fault Reporting Module:* records and forwards fault reports, also known as network trouble tickets, to trouble ticket and other systems.

g. *Trouble Ticket System*: stores trouble ticket information including the root cause of the problem along with other relevant information. This information includes trouble resolution time, resource information, link information and information about the type of service affected. The information is updated every time a new information is received from the fault reporting module.

h. *Fault Archive Module:* stores information about alarms (events plus user operation logs) and trouble tickets creation and management, including information from operation and maintenance team.

As shown in Figure 2, the automated or self-learning RCA system takes additional information from various data sources such as trouble ticket system (RCA history), alarm rule engine, and different elements and network management systems. The architecture also shows feedback loop for making root cause analysis. The loop is periodically executed in order to search and learn new rules from previous fault archives from which the respective root causes have been identified manually by domain experts. The output of the classifier module is combined with the alarm engine rule in one rule which is used to dynamically associate related alarms and select the root cause from a set of related alarms.

4. Experimental Results

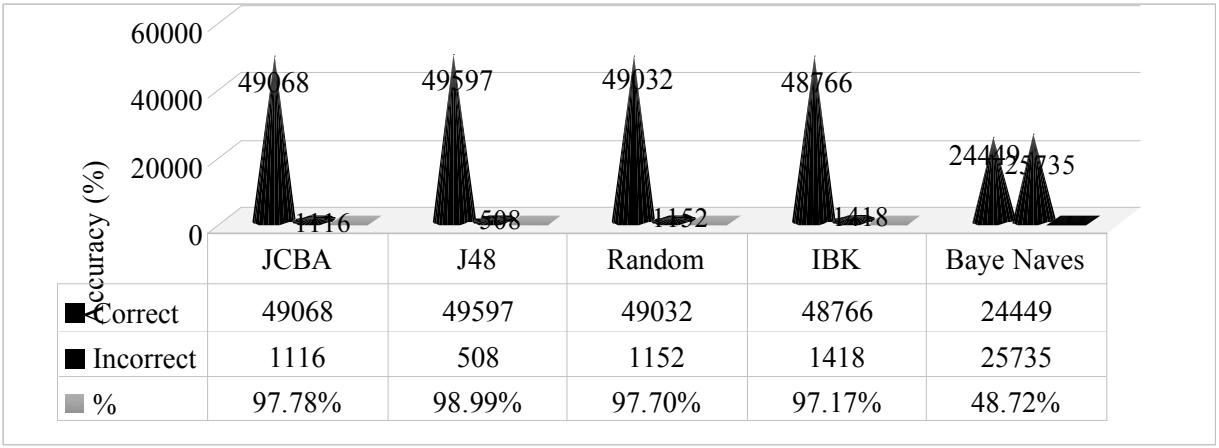
We performed two experiments to assess the effectiveness and efficiency of the proposed approach using five different algorithms: JCBA, J48,

Random Forest, IBK, and Naïve Bayes. These algorithms are selected due to the fact that they are widely used and in addition they belong to four different families of learning algorithms; association rule-based learners, instance-based learners, probabilistic-based learners and decision tree learners. Besides to this, many researches [6, 12, 13] on fault management, RCA and machine learning include one or more of these algorithms and they are all discussed extensively in many literatures.

The experiments are conducted using an HP ProLiant DL380 server (with 8 GB memory), Weka 3.8.2 tool, which is a popular suite of machine learning software written in Java, developed at the University of Waikato, New Zealand [14] and using 100,000 pre-processed alarm instances collected from five different technologies namely, transmission, power, IP, mobile core, and access domains.

The first experiment is conducted using 50,184 training dataset and 10 cross validation test options. Its purpose is to examine the effectiveness or accuracy of the selected algorithms for RCA. Figure 3 shows the result of the selected classifiers on the basis of correctly and incorrectly classified instances. As it can be seen, different algorithms gave different results. The lowest accuracy was achieved by Naïve Bayes (48.72%), followed by IBK (97.17%) and Random Forest (97.70%), respectively. Most likely, such a bad accuracy is the result of having high dependability between features. In our case, most of the faults are interrelated or correlated to one another and this is the most probable reason of a bad result of the Naïve Bayes algorithm. The highest accuracy was achieved with the J48 and JCBA algorithms with values of 98.83% and 97.77%, respectively.

The second experiment is performed using the first training dataset and five other derived test sets. Its main purpose is to verify the selected algorithms can be used for real-time or near real-time fault root cause analysis. For each test case, three experiments are performed: each time the testing time is recorded. Figure 4 shows the overall average result of the experiments.



	JCBA	J48	Random	IBK	Baye Naves
Correct	49068	49597	49032	48766	24449
Incorrect	1116	508	1152	1418	25735
%	97.78%	98.99%	97.70%	97.17%	48.72%

Figure 3: Result of Classifiers on the Basis of Correctly and Incorrectly Classified Instances

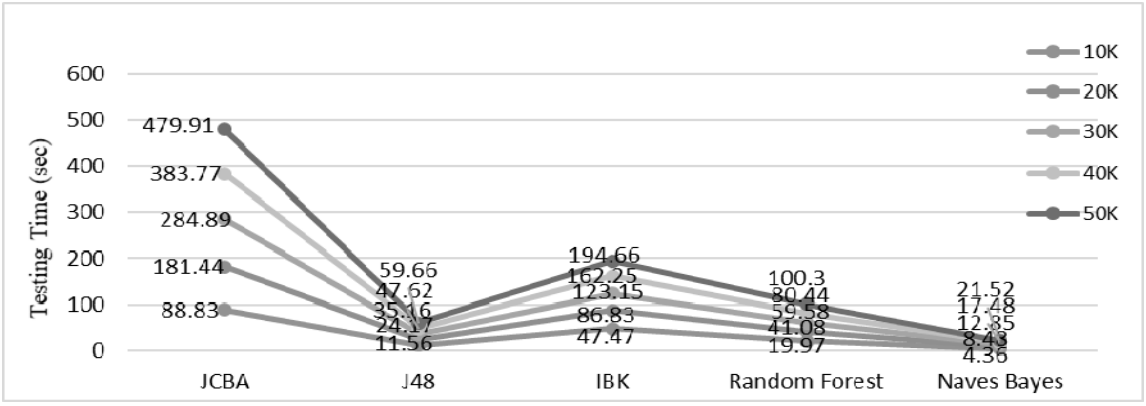


Figure 4: Comparison of Classifiers on the Basis of Response Time Measure

As can be seen from Figure 4, the result achieved by Naïve Bayes is much better than others, followed by J48. Random Forest is in the third place with an average response time of 20 seconds, while IBK and JCBA were ranked fourth and fifth with response time of 48 and 89 seconds for 10,000 datasets, respectively.

5. Evaluation

To evaluate the performance of the selected classifiers, we used F1 score, ROC area, overall accuracy and 10-cross validation measures. These metrics are selected based on their applicability for multi class problem, invariance to imbalanced class [15, 16] and simplicity to understand. Table 1 shows the comparison between J48, JCBA, Random Forest, IBK and Bayes Navies classifiers on the basis of F1 score, ROC area, precision, and recall measures.

The first evaluation measure used is F1 score, which is the harmonic mean value of precision and recall. According to the results in Table 1, J48 gave a greater level of precision (0.98) than the others, producing a smaller number of false positive instances. Furthermore, J48 outperformed the others in terms of the recall measure, i.e., the number of correctly classified instances is greater than the number of false negative instances, which is equivalent to the accuracy measure. The lowest F1 value is scored by Naïve Bayes, producing a large number of false positive and negative values.

Table 1: Evaluation of Classifiers based on Different Measures

Classification Model	*TP Rate*	*FP Rate*	*Precision*	*Recall*	*F1-Score*	*ROC Area*
J48	0.980	0.007	0.981	0.980	0.980	0.995
JCBA	0.972	0.01	0.972	0.972	0.972	0.992
Random Forest	0.977	0.008	0.977	0.977	0.977	0.991
IBK	0.978	0.008	0.978	0.978	0.978	0.987
Naïve Bayes	0.487	0.171		0.487		0.735

The second evaluation measure used is area under ROC curve (AUC), which is a trade-off between the true and false positive rates. According to the results in Table 1, J48 gave a greater level of TP and FP rates than the others. Overall, the AUC value of JCBA, Random Forest, and IBK classifiers do not have any significant differences with each other whereas Naïve Bayes performed the lowest AUC value, which is 0.735.

The third evaluation metric is overall accuracy, which is calculated as the ratio of true instances and the total number of instances examined. We used this metric to discriminate classifiers based on their computational cost and complexity. Figure 5 presents a summary of J48, JCBA, Random Forest, IBK and Naïve Bayes classifiers based on overall accuracy measure, with J48 outperforming the other four with overall average accuracy of 98.04%. This means that J48 is more accurate and effective in identifying all class instances than the other classifiers. JCBA,

Random Forest, IBK and Naïve Bayes were less accurate and ranked from the second to the fifth positions with an overall accuracy of 97.77%, 97.70%, 97.174% and 48.72%, respectively.

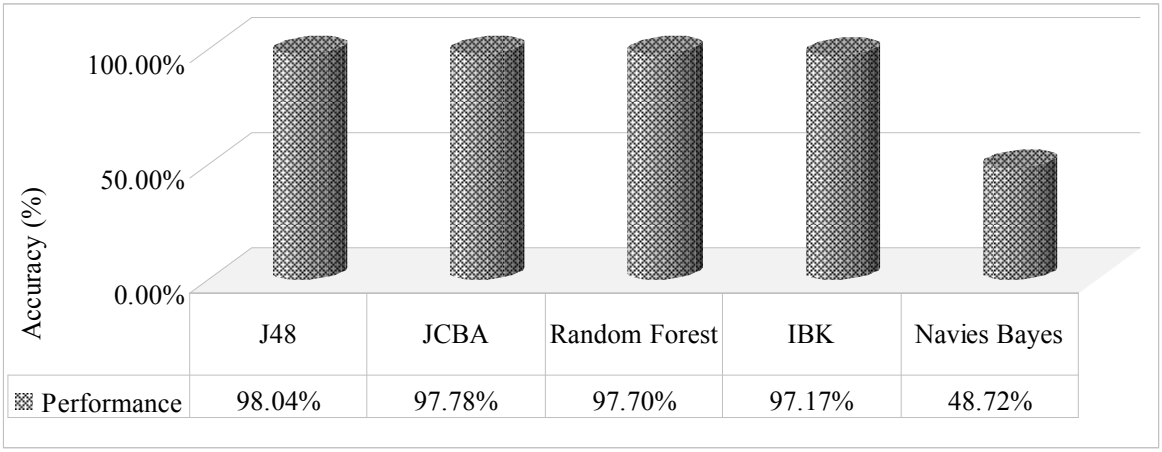


Figure 5: Evaluation of Classifiers Based on Overall Accuracy Measure

To summarize, the main function of a root cause analysis (RCA) system is to identify the cause of a problem from a set of interrelated faults in order to provide valuable information to telecom operators and resume interrupted services within the agreed SLA (Service Level Agreement) time. With this context, decision tree algorithms have identified faults accurately and precisely within the required time frame than others.

6. Conclusion and Future Work

In this paper, we presented a solution for RCA of a multi-domain and heterogeneous network using a self-learning approach. The solution consists of two modules: alarm rule engine module which consists of known business rules defined by domain experts and vendors, and machine learning module, which is responsible for leaning new rules from previous fault archive. Finally, the output of each module is combined into one rule which is used to dynamically associate related alarms and select the root cause from a set of related alarms called symptom alarms.

This solution does not require expert knowledge, except during the pre-processing phase, as once the pre-processing is done, the same features can be used for RCA, which is one certain advantage as compared to the traditional rule-based classification approaches, where threshold values need to be adjusted by experts every time a new product and technology is introduced to the network. One more benefit is that, once the training data is ready, the machine learning model developed can be used as a black-box approach to RCA.

The following are future works.

- This work is tested on telecommunication network and further research will be done using other similar infrastructures such as IT data centers.
- Because of hardware limitation, Artificial Neural Network (ANN) algorithms are not included in this work and further research will be conducted using these algorithms.

References

[1] S. Małgorzata and S. Adarshpal, "A Survey of Fault Localization Techniques in Computer Networks," Watson Research Center, Hawthorne, Vol. 53, No. 2, pp. 165-194, 2004.

[2] H. Jinqiu, C. Shuang, and Z. Laibin, "Alarm Management Technology and its Progress in Process Industries," in 2nd International Conference on Control, Automation, and Artificial Intelligence (CAAI 2017), Beijing, 2017.

[3] A. Mazdziarz, "Alarm Correlation in Mobile Telecommunications Networks based on K-means Cluster Analysis Method," pp. 95-102, 2018.

[4] J. Ahnlund, T. Bergquist, and L. Spaanenburg, "Rule-based Reduction of Alarm Signals in Industrial Control," in IEEE International Conference on Emerging Technologies and Factory Automation, Sweden, 2018.

[5] T. Saha, H. Rangwala, and C. Domeniconi, "Active Learning for Relational Network Classification," pp. 1-16, 2014.

[6] E. Rozaki, "Network Fault Diagnosis Using Data Mining Classifiers," Computer Science & Information Technology (CS & IT), pp. 1-12, 2015.

[7] E. Rozaki, "Design and Implementation for Automated Network Troubleshooting Using Data Mining," International Journal of Data Mining & Knowledge Management Process (IJDKP), Vol. 5, No. 3, pp. 1-19, 2015.

[8] P. Singh and S. Verma, "An Efficient Software Fault Prediction Model using Cluster based Classification," International Journal of Applied Information Systems (IJAIS), Vol. 7, No. 3, pp. 1-7, May 2014.

[9] Markus Felldin, "Machine Learning Methods for Fault Classification," pp. 1-48, 2014.

[10] R. Eleni, "Network Fault Diagnosis Using Data Mining Classifiers," Computer Science & Information Technology (CS & IT), pp. 1-12, 2015.

[11] S. S. Gosavi, "Machine Learning Methods for Fault Classification," pp. 1-72, 24 April 2014.

[12] I. K. O. K. Denise W. Gurer, "An Artificial Intelligence Approach to Network Fault Management," pp. 10-19, January 2016.

[13] M. Felldin, "Machine Learning Methods for Fault Classification," pp. 1-48, 2014.

[14] "Weka 3: Machine Learning Software in Java," 2018, Available at: https://www.cs.waikato.ac.nz/~ml/weka/, Accessed on 27 May 2018.

[15] A. Tharwat, "Classification Assessment Methods," Applied Computing and Informatics, Vol. 7, pp. 1-13, 21 August 2018.

[16] H. Mohammad and S. Nasir, "A Review on Evaluation Metrics for Data Classification Evaluations," International Journal of Data Mining & Knowledge Management Process (IJDKP), Vol. 5, No. 2, pp. 1-11, 2015.

[17] N. R. Babu and B. J. Mohan, "Fault Classification in Power Systems using EMD and SVM," Ain Shams Engineering Journal, Vol. III, No. 103, pp. 103-111, 2017.

[18] M. Awad and R. Khanna, “Efficient Learning Machines: Theories, Concepts, and Applications for Engineers and System Designers”, Apress, 2015.