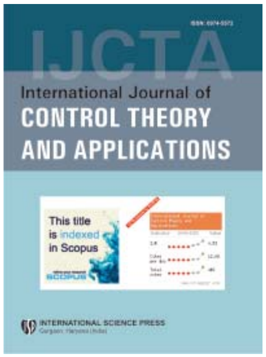

International Journal of Control Theory and Applications

ISSN : 0974–5572

© International Science Press

Volume 10 • Number 27 • 2017

# A Novel Approach to IDS using Layered Mutual Information Feature Extracted CRF

**S. Vinila Jinny[a] J. Jaya Kumari[b] and S. R. Surem Samuel[c]**

[a]*Assistant Professor, Department of Computer Science and Engineering, Noorul Islam University, Kumaracoil.*

*E-mail: vinijini@gmail.com*

[b]*Head of the Department, Department of Electronics and Communication Engineering, Noorul Islam University, Kumaracoil.*

*E-mail: jkumaribharat@yahoo.com*

[c]*Assistant Professor, Department of Electronics and Communication Engineering, CSI Institute of Technology, Thovalai.*

*E-mail: suremsam81@yahoo.co.in*

***Abstract:*** As network usage increases daily, it became a part of our life. So it is necessary to provide security to avoid problems in our real time requirements met by this. Providing Security is very easy when the flaw and its cause are known. Here comes the difficulty, damage caused to the system is known but can't able to find the cause. So we need analysis methods to identify the cause of the flaw. Data mining is a technique by which the fact that exists in the data can be extracted. Intrusion Detection System is a system that detects the intrusion by using intrusion and normal behaviour patterns. In this system, generating pattern is the major work, which affects the performance of the intrusion detection system. When the pattern generated is the best, and then the Intrusion Detection System accuracy will be high. For extracting the best patterns data mining techniques can be applied. Earlier many methods like decision tree, support vector machine, Bayesian classifiers are used, which also provided better accuracy. But the performance is low, because increase in computation time and space usage. The performance can be improved by performing an additional step of pre-processing, which helps to remove redundant features and less influenced features. It helps in reducing computation time and space used, which ultimately improves the performance of the system. In this paper, a novel approach is used. A classification model is generated using Conditional Random Field based classifier, which takes in a pre-processed set features created by mutual information feature selection method and this model is split in to layers based on the categorization of attacks. The proposed method is tested with KDD CUP 1998 dataset and real time dataset, which show improvement in performance and detection accuracy than the existing systems.

***Keywords:*** *Intrusion Detection System, Data mining, Conditional Random Field, Classifier, Mutual-information.*

## 1. INTRODUCTION

As network usage increases day by day, hackers too have been increased to a large extent. These intruders show their ability on highly protected networks with firewall. When we study about those incidents some 40% knows where they have been attacked but some 30% don't know where they have been attacked. So there is a requirement of analysis of previous to study about place and concept of attack. So, many of the vendors, enterprises and most of the organisation are waiting for a better solution that solves this intrusion problem. The first source of security protection given for networks is firewall, which filters packet based on packet header information. Also most of intrusion detection systems also filters network based on packet header information. So there is a requirement that take a step forward to monitor the inner content of the packet. Advanced intrusion detection system performs better content analysis of the packet. Because of this ability it became the major requirement for the network to provide security. The IDS systems may be provided outside or inside of the firewall protected networks.

Based on the deployment of IDS in network, it is categorised in two: Host based and network based [1]. Host based monitors a particular system by using event log, whereas network based monitors the network traffic for possible suspicious activity. IDS systems can also be categorised based on the detection technique. This includes Known attack detection, Unknown attack detection and network overloading detection. Known attack detection is known to be Signature Detection, Unknown attack detection is known to be Anomaly detection and network overloading detection is known to be Denial of Service detection. With any one of the above techniques alone may not be sufficient for efficient intrusion detection system. To make an efficient system, it is necessary either to embed these techniques or develop a technique that uses hybrid concept of these techniques.

The main challenge today is to develop a system that accurately detects the intrusion. To accurately detect, it is necessary to have better coverage of intrusion signatures. In this paper a novel approach is explained which makes changes in the three modules of Data Analysis part of IDS. Mutual Information of features are used to select the best features. With that feature set the Classifier is generated using Conditional Random Field. This Classifier is generated in four layers by performing an attribute selection so that the time for search is highly reduced. The Remaining part of the paper is organized as follows: Literature Survey explains the details of existing systems. Next section explains the overview of IDS. Proposed Work explains the methodology. Next Section gives the flow of the work and its performance. Results section deals with performance analysis and its discussion. Final section comes with the conclusion.

## 2. LITERATURE SURVEY

When we search and learn about IDS systems, analysis module plays an important role in improving the accuracy and performance of the system. It is been said that accuracy of the system is improved by generating a good classifier model. Lumbomir et al.,[3] suggests a new classifier that combines the supervised and unsupervised model. Here it uses adaptive resonance theory network for unsupervised model. Linear Discriminant Classifier is used for supervised model. This Linear Discrminant Classifier classifies both normal and intruded behaviour. This shown better performance over back propagation network.

Though classifier models are designed using best classification algorithms it is been found that applying a feature selection highly reduced the training time in developing a classification model. P. Ravisankar et al.,[5] tells that on testing various data mining techniques such as Multilayer Feed Forward Neural Network (MLFF), Support Vector Machines (SVM), Genetic Programming (GP), Group Method of Data Handling (GMDH), Logistic Regression (LR), and Probabilistic Neural Network (PNN) to identify companies that resort to financial statement fraud, found PNN is best without feature selection and both PNN and GP performs well with feature selection.

After generating a classifier model, it can be optimized to get good result. Oliver et al.,[4] tells about the use of Evolutionary Algorithms for optimization of a Radial Basis Function Network. Wenying et al., [6] tells a newly optimized clustering technique called Clustering based on Self-Organized Ant Colony Network. Here it outperforms the performance of Support Vector Machine. Final result is improved much by combining Support

Vector Machine with above said optimization. M.N. Mohammad et al., [7] tells that combining the ready-made data mining algorithms produces good accuracy in detection and has tested using the weka data mining tool. R.M. Elbasiony et al. [8] suggests a hybrid intrusion detection system, which uses random forest algorithm for misuse detection and weighted K-means clustering for anomaly detection and evaluated with KDD'99 data set and got better detection rate and false positive rate. Most HU et al., [9] suggests a novel approach that meets the drawback adaptability, which is a known issue not considered by most of the researchers. As network environments are changing frequently, it is an important issue to be tackled. Two online Adaboost-based algorithms are proposed. Weak classifier Gaussian mixture models are used. Local model and global model together performs well to detect the intrusions. Biggio et al., [10] proposed a system that secures the classification model of the IDS. If classification model is compromised the whole IDS is ruined. Here that issue is tackled by checking the classifier on each updating, which prevents the locking of IDS. Hannes [11] proposed a novel technique to identify the time taken for future intrusion. It is been said that time taken for future intrusion follows poisson distribution. Ismail et al., [12] made a study of IDS in wireless sensor networks. In Mobile Adhoc Networks IDS vulnerability is high and can be tackled by mining methods or machine learning methods.

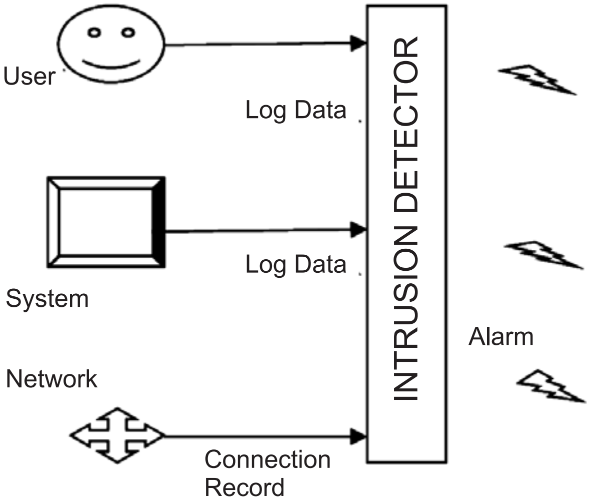

**Figure 1: Intrusion Detection System**

## 3. OVERVIEW OF IDS

Fig.1 depicts the overall construction of an intrusion detection system. Intrusion Detection system helps to identify abnormal behaviour found in network log, system log and user log. In order to identify the abnormality the detector module is set with patterns that represent the intrusive behaviour and normal behaviour. Based on the deployment [2] of IDS, it is classified into two types: Host-Based IDS and Network Based IDS. The Techniques used in IDS includes two types signature detection and anomaly detection. In Signature Detection the known intrusion patterns are packed in a database.

## 4. PROPOSED WORK

The proposed work is concentrated towards the classification module of the intrusion detection system. The classification model is generated with four categories of intrusions. KDD'99 CUP standard is used to evaluate the classifiers of intrusion detection systems. Relevance of the features of the dataset for detection is considered in feature selection phase. Mutual Information is considered for selecting the features. The proposed system is a hybrid system that performs both misuse detection and anomaly detection.

### 4.1. KDD, 99 Cup Dataset

KDD'99 CUP dataset is a standard dataset widely used to develop and test classifiers of intrusion detection systems. There are about 494,021 records in the training dataset, which consists of 97,277 normal records *i.e.*, 19.69% normal records, 391,458 DOS intruded records *i.e.*,79.24% DOS intrusion, 4,107 Probed records *i.e.*, 0.83% Probe intrusion, 1,126 Remote to Local intruded records *i.e.*, 0.23% R2L intrusions and 52 User to Local intruded records *i.e.*, 0.01% U2L intrusions. Each connection records contains about 41 features which describes the connection. A Label is used to assign intrusion or normal.

The training dataset consists of about 22 different attacks and test dataset consists of about 39 different attacks. Attacks found in the training dataset is considered as the known attack and the attack found in the test dataset is considered as the novel attacks. The categorization of intrusion is as follows:

1. Denial of Service Intrusion
2. User to Root Intrusion
3. Remote to Local Intrusion
4. Probe intrusion

Denial of Service Intrusion is a type in which the required resources of the users is made busy by either linking server to unwanted access or make the network connecting the server too traffic. Some of the examples of Denial of Service intrusion were 'neptune', 'teardrop', 'back', 'land', 'smurf' and 'pod'. User to Root intrusion is a type in which the normal user tries to gain the rights of a server. Here the system stays as normal user for a particular period and then slowly gains access of the root. Examples of such type of intrusions include, 'perl', 'buffer overflow', 'root kit' and 'load module'. Remote to Local intrusion is a type in which an unknown host from remote places tries to gain access of a particular system and then exploiting the resources of the local host. Example of such intrusions include 'phf', 'warez client', 'ftp_write', 'multihop', 'guess_passwd', 'warez master', 'imap' and 'spy'. Probing is a type of intrusion, in which any host at any network is intruded to achieve either information or rights or stop the resources. This type includes 'nmap', 'portsweep', 'ipsweep' and 'satan'.

### 4.2. Feature Selection

Feature selection is a process in which, set of features are taken and processed to produce a subset that affects the output effectively and are more interesting to improve accuracy and reduce unnecessary computation time. Feature selection methods are categorised in to filter approach and wrapper approach.

#### *4.2.1. Mutual Information based feature selection algorithm*

This algorithm focuses on selecting attributes that distinctively involve the output. It performs two calculations.

1. Mutual value between class labels and features
2. Mutual value between features

**The Algorithm flow follows the steps as said below :**

1. Create Three Lists A, B, C.
2. Assign initial value to the sets A, B, C
   a) A-first set of features
   b) B-Null set
   c) C-class outputs

3. Compute the mutual value between class label and feature. Repeat the step for all features with class label.
4. Give Rank to the features based on the mutual value calculation.
5. Include high mutual value features to B.
6. Revise List A by excluding selected features.
7. Repeat the steps 3-6 until required number of features are selected.
8. Now compute mutual value between features itself. *i.e.*, features selected and features not selected.
9. Consider the features whichever has high mutual value.
10. List B is considered the final set of selected features.

## 4.3. Classification Model

Generating classification model is the mainly concentrated area of this work. Classification is a technique in which a new label is assigned to unlabeled patterns. Classification can be done in two ways: First labels are decided and then patterns are grouped based on the required attribute of the label. In the Second way groups are formed with similar attributes and the labels are suggested for each group. Second way of classification is called as clustering. Classification is supervised way of training the system whereas clustering is unsupervised way of training the system. To develop the Classification model Conditional Random Field method is used. CRF implementation performs the following steps.

1. Network data as categorical features are taken as input based on the feature selection.
2. Perform decoding by viterbi algorithm.
3. Make the inference with forwards-backwards algorithm.
4. Sample the pattern using forwards-filter backwards-sample algorithm.
5. Use limited-memory quasi-Newton algorithm for parameter estimation.
6. Patterns for anomaly are updated to the data base.

## 4.4. CRF-Classification Model

CRF is Conditional Random Field, which comes under the category of statistical modelling technique. Mostly used in pattern recognition and machine learning research area.CRF is a supervised machine learning technique, which performs structured prediction. Classifiers classify a sample to its corresponding label by comparing the features. CRF also performs the same but while in classification it takes account of neighbouring samples. CRF is a type of undirected discriminative probabilistic graphical method. It constructs consistent interpretations by encoding the known facts between observations. Lafferty, McCallum and Pereira defined a CRF on observations A and random variables B as follows:

Let G = (V, E) be a graph such that $B = (B_v)_{v \in V}$, so that B is indexed by the vertices of G. Then (A,B) is a Conditional Random Field when the random variable $B_v$, conditioned on X, obey the markov property with respect to the graph.

$$p(B_v \mid A, B_w, w \neq v) = p(B_v \mid A, B_w, w \sim v) \tag{1}$$

Where $w \sim v$ says that w and v are neighbours in G.

### 4.5. Multi-level Classification Model

As the attack is classified in to four categories, the classification level is also set to four.

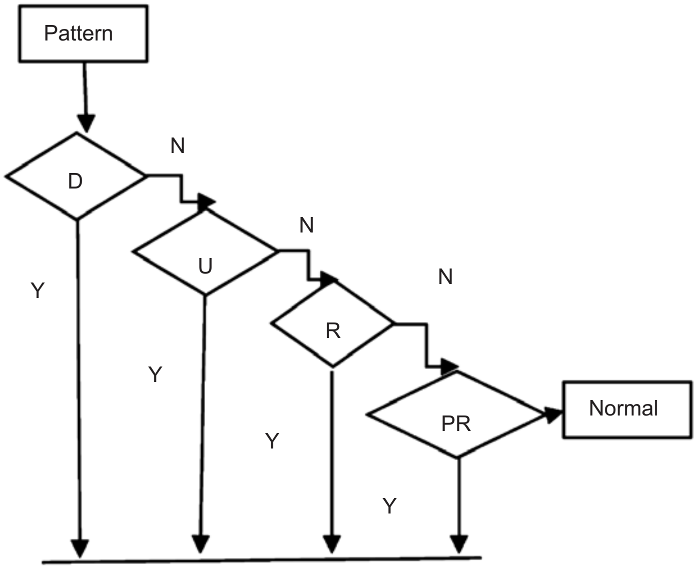

**Figure 2: Layered Classification Modules**

The First layer detects all types of attacks of Denial Service Type, then the data goes through the next layer in which all characters with User to Root intrusion is identified and restricted, next layer scans for all Remote to Local Intrusions and then finally identifies for Probe intrusion. In each layer features specific to given intrusion type is verified, so that unnecessary scanning of full data is highly reduced.

## 5. PERFORMANCE EVALUATION

The IDS is measured based on its accuracy and specificity of detection. Accuracy is how able the system is to detect the signature. Statistical measures of classification are Sensitivity and Specificity. Sensitivity is also named as true positive rate or recall rate, which measures the ability of system to identify truth correctly. It is opposite to false negative rate. Specificity is also named as true negative rate, which measures the ability of system to identify false correctly. It is opposite to false positive rate. A system having 100% specificity and 100% sensitivity provides high accuracy.

## 6. RESULTS AND DISCUSSION

### 6.1. Feature Selection Output

Network data [16] is taken as input to the feature selection module. This module uses mutual information between features and between feature and label. Based on the mutual information 42 features are ranked. A threshold value is set to screen out the uninfluenced features to the output. When the threshold value is increased most of the features are eliminated that much influences output. When the threshold value is lowered feature selection has no effect. A better threshold is set so that necessary features are not omitted and unnecessary features are set out. Table 1. represents the features when selected with various threshold levels. Table 2 gives the accuracy of the system when tested with single classification module, after applying mutual feature selection algorithm, with layered classification. Table 3 and 4 gives the performance evaluation and time taken by the system for anomaly detection. Figure 3,4 and 5 shows the table values with graphical presentation.

**Table 1**
**Features selected with various threshold value**

| *Threshold value* | *No. of features Selected* |
|---|---|
| 0.45 | 0 |
| 0.4 | 1 |
| 0.35 | 2 |
| 0.3 | 5 |
| 0.25 | 8 |
| 0.2 | 10 |
| 0.15 | 11 |
| 0.1 | 17 |
| 0.05 | 30 |
| 0.01 | 39 |
| 0 | 41 |

**Table 2**
**Detection Accuracy**

| *Classification Algorithm* | *Accuracy of detection (in %)* | |
|---|---|---|
| | *Correctly classified* | *Incorrectly classified* |
| CRF | 90.4 | 9.6 |
| Mutual Feature CRF | 93.8 | 6.2 |
| Mutual Feature Layered CRF | 95 | 5 |

**Table 3**
**Performance Evaluation**

| *Classification Algorithm* | *Accuracy of detection (in %)* | |
|---|---|---|
| | *Training time* | *Testing time* |
| CRF | 5.73 | 2.2 |
| Mutual Feature CRF | 4.1 | 1.5 |
| Mutual Feature Layered CRF | 2.2 | 0.5 |

**Table 4**
**Accuracy comparison with time**

| *Classification Algorithm* | *Test Accuracy* | *No. of features* | *Model building time (in secs.)* |
|---|---|---|---|
| CRF | 90.4 | 41 | 7.93 |
| Mutual Feature CRF | 93.8 | 24 | 5.6 |
| Mutual Feature Layered CRF | 95 | 8 | 2.7 |

## 7. CONCLUSION AND FUTURE ENHANCEMENT

The Accuracy of the intrusion detection system is most important that affects the whole system. Accuracy of the system can be improved in various ways. One such challenge available is selecting a best classifier to form best patterns to prevent missing horrible poisons. Though classifier is selected it may have some difficulties to achieve the sharpness. Classifier considered here is conditional random field which is sharpened by providing best features by mutual information feature selection approach. The computation time is highly reduced by layering the detection modules based on attack category. The system can be further improved by selecting classifier specific to attack category and applying in each layer. Research proceeds with this future plan and also the security of the classifier module is also at risk so it is needed to add authentication module.

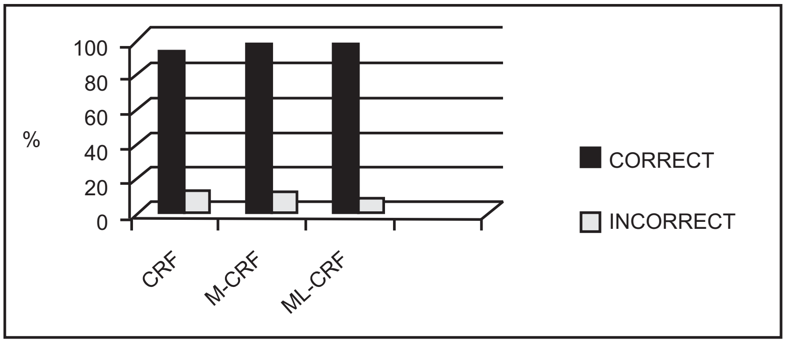

**Figure 3: Detection Accuracy**

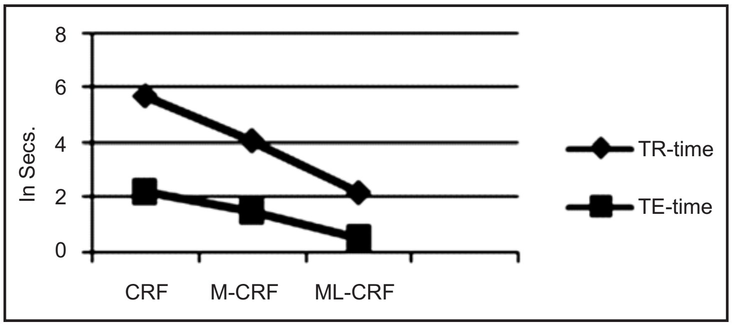

**Figure 4: Performance Evaluation**

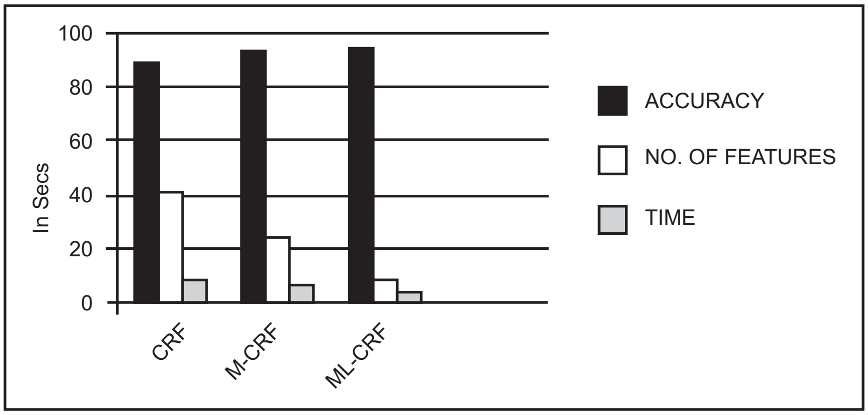

**Figure 5: Accuracy Comparison with time**

## REFERENCES

[1] Dr. Fengmin Gong, “Next Generation Intrusion Detection Systems (Ids)”, *Network Associates*, March 2002.

[2] Monowar H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “Network Anomaly Detection: Methods, Systems and Tools”, *IEEE Communications Surveys & Tutorials*, Vol.16, pp. 03-336, 2014.

[3] Lubomir Hadjiiski, Heang-Ping Chan, Nicholas Petrick and Mark Helvie, “Classification Of Malignant And Benign Masses Based On Hybrid Art2lda Approach”, *IEEE Transactions On Medical Imaging*, Vol.18,1999.

[4] Oliver Buchtala, Manuel Klimek, and Bernhard Sick, “Evolutionary Optimization Of Radial Basis Function Classifiers For Data Mining Applications”, *IEEE Transactions On Systems, Man, And Cybernetics—Part B: Cybernetics*, Vol.35, 2005.

[5] P. Ravisankar , V. Ravi , G. Raghava Rao and I. Bose, “Detection Of Financial Statement Fraud And Feature Selection Using Data Mining Techniques”, *Decision Support Systems*, Vol.50, pp.491–500, 2011.

[6] Wenying Feng, Qinglei Zhang, Gongzhu Hu and Jimmy Xiangji Huang, “Mining Network Data For Intrusion Detection Through Combining Svms With Ant Colony Networks”, *Future Generation Computer Systems*, Vol.37, pp.127–140, 2014.

[7] Muamer N. Mohammad, Norrozila Sulaiman and Osama Abdulkarim Muhsin, “A Novel Intrusion Detection System By Using Intelligent Data Mining In Weka Environment”, *Procedia Computer Science*, Vol.3, pp.1237–1242, 2011.

[8] Reda M. Elbasiony, Elsayed A. Sallam, Tarek E. Eltobely and Mahmoud M. Fahmy, “A Hybrid Network Intrusion Detection Framework Based On Random Forests And Weighted K-Means”, *Ain Shams Engineering Journal*, Vol.4, pp.753–762, 2013.

[9] Weiming Hu, Jun Gao, Yanguo Wang, Ou Wu, and Stephen Maybank, “Online Daboost-Based Parameterized Methods For Dynamic Distributed Network Intrusion Detection”, *IEEE Transactions On Cybernetics*, Vol.44, 2014.

[10] Battista Biggio, Giorgio Fumera, and Fabio Roli, “Security Evaluation Of Pattern Classifiers Under Attack”, *IEEE Transactions On Knowledge And Data Engineering*, Vol.26, 2014.

[11] Hannes Holm, “A Large-Scale Study of the Time Required to Compromise a Computer System”, *IEEE Transactions On Dependable and Secure Computing*, vol.11, 2014.

[12] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, “A Survey of Intrusion Detection Systems in Wireless Sensor Networks”, *IEEE Communications Surveys & Tutorials*, vol.16, 2014.

[13] Monowar H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “Network Anomaly Detection: Methods, Systems And Tools”, *IEEE Communications Surveys & Tutorials*, vol.16, 2014.

[14] Adetunmbi A.Olusola., Adeola S.Oladele. and Daramola O.Abosede, “Analysis Of Kdd ’99 Intrusion Detection Dataset for Selection of Relevance Features”, *Proceedings of the World Congress on Engineering and Computer Science*, vol.1, 2010.

[15] Emmanuel S. Pillai, R.C. Joshi and Rajdeep Niyogi, “Network forensic frameworks: survey and research challenges”, *Digital Ivestigation*, vol.7, pp.4-27, 2010.

[16] D.Barbara, S.Jajodia, “Applications of Data Mining in Computer Security”, 2002.

[17] S. Vinila Jinny and J. Jaya Kumari, “Comparitive analysis of Intrusion Detection Systems with mining”, *International Review on Computer Software*, vol.8,pp.2541-2544, 2013.

[18] S. Vinila Jinny and J. Jaya Kumari, “Encrusted CRF in intrusion Detection System”, *Advances in Intelligent and Soft Computing,* Springer, vol.325, pp.602-614, 2015.