International Journal of Computer Networks and Communications Security

VOL. 5, NO. 4, APRIL 2017, 76–82
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Proposing A New Model to Improve Alert Detection in Intrusion Detection Systems

Behrooz Shahi Sheykhahmadloo[1] and Samira Mehrnoosh[2]

[1] Master of Software Engineering, Department of Computer Engineering, University of Isfahan, Isfahan, Iran

[2] Master of Software Engineering, Department of Computer Engineering, University of Shiraz, Shiraz, Iran

[1]sheykhahmadloobehrooz@gmail.com, [2]samira.mehrnoosh@gmail.com

ABSTRACT

Using Intrusion Detection Systems is essential in today's systems to detect cyber attacks. IDS identify undesirable behaviors by getting information from systems that are under their surveillance and give them to network analyst as an Alert. A summary view of network security status is obtained by clustering and labeling alerts. Detection and quality of alerts are the two primary challenges of these systems. The number of IDS alerts is too much that the network analyst can't survey all of them. In this article, a method has been presented in which the above mentioned shortcoming will be reduced by semantic expansion of alerts' information. We will show that semantic expansion of alerts' information based on background knowledge before clustering step leads to a much better clustering. DARPA dataset is used to evaluate the proposed method. Alerts' detection rate will be more than 96%, which is better than similar approaches.

Keywords: *Semantic Expansion of Alerts, Clustering Alerts, Intrusion Detection Systems*.

1 INTRODUCTION

Due to the widespread use of the Internet, internet attacks and unauthorized intrusions in recent years have grown substantially. Intrusion Detection Systems have been introduced to identify and reduce unauthorized intrusions. These systems identify undesirable behaviors by investigating network traffic and systems' status. Then, give their output as an "Alert" to network analyst but there are two reasons that show most of the time, this output is not very useful for the network analyst. First, the number of these alerts is too much that the network analyst cannot investigate them. Intrusion Detection Systems (IDS) usually produce thousands of alerts everyday [1]. Second, according to the surveys conducted, a large volume of alerts are false positive [2].

Some methods have been introduced to achieve the goals of correlation systems. The result of analyzing these methods shows that each of these methods only covers some of the goals of correlation process and the results of each method cannot be used in other methods. For example, in the correlation method based on clustering, logged in security alerts are classified according to similarity measures that their aim is reducing alerts and recognizing the sequence of attacks, while this method cannot detect false positive alerts. The main root of expressed problem is that most of these systems use from initial information of security alerts which have very low semantic level. Using these initial and low level information expectations of these systems are not satisfied. Therefore, to improve such systems expanding information of security alerts and increasing their semantic level are essential. The method proposed in this article is two-level architecture. In the first stage of the proposed architecture, using the information of Intrusion Detection Systems and meaningful information of TableExpand table, alerts are converted to expanded alerts with use of the proposed algorithm. In the next section, using expanded alerts, an algorithm is introduced for clustering expanded alerts with comparing the similarity between alerts' features.

The article is organized as follows: Previous and related works are discussed in section 2. In Section 3, we introduce a new architecture for correlation system and describe this architecture. In section 4, we show the results of experimental evaluation and comparison with previous works. And finally the last section concludes this article and introduces future works.

2 THEORETICAL BACKGROUND

In recent years, the use of correlation for alerts of Intrusion Detection Systems has become prevalent. According to algorithm type, correlation approaches can be divided into three groups [5, 6]:

1. Approaches based on similarity measuring between alerts.
2. Using of knowledge base.
3. Approaches based on statistical information.

In approaches based on similarity measuring, consider criteria to compare similarity rate of two alerts or one alert or a group of alerts that if an alert has the similarity, it will be put in the related group and if the alert doesn't have similarity to any group, it will be put in the new group. In statistical approaches by using of statistical analysis of previous data, causal relationships between different alerts are recorded and frequency of their occurrence is analyzed and sequences of attacks are made. In approaches based on knowledge base, there is an alert and attack base in it, in which systems are analyzed by using of this information.

Analysis done by QIN [7], in 2005, is one of the best and most prominent approaches which are based on statistical analysis. This approach correlates to identify attacks that have an attack scenario. First, security alerts as input are classified and then based on attacks' communication and effect on the goal are prioritized. Finally, attack scenarios can be constructed by using of causal analysis.

Ning [8, 9] implemented alerts' communications with prerequisites and outcomes. This approach is based on knowledge base and prerequisites and outcomes are in knowledge base. According to it, alerts' graph is generated and analysis is done. This approach works offline.

In another study done by Dain and Cunningham [10, 11], they tried to classify alerts by using of machine learning techniques. In this algorithm, alerts manually have been divided into a number of scenarios and the purpose is training a system to learn an appropriate model for clustering alerts by using these scenarios.

Smith and his colleagues [12,13,14], presented another approach for clustering. Inputs of their system are Snort alerts and output is a criterion for the similarity between two alerts. They use from neural network technique for comparison.

Another approach based on similarity measuring has been done by Valeur and his colleagues [15, 16] in 2004 and 2006.This algorithm has the most components division and is more similar to Valdes algorithm. An important difference between this algorithm and Valdes algorithm is that in Valdes algorithm alerts are kept in main memory and each new alert is compared with available alerts of higher levels which are called" meta alert" and alerts are classified. But in Vigna algorithm is defined a time window. The alerts that are not generated or updated during set time will be removed from memory and processing.

In research, done by Julisch [2,3,17] and his colleagues, the purpose of analyzing the security alerts is to find basic reasons of alerts. The input of their system is a series of security alerts and output is hierarchical and meaningful classification of security alerts which are system's inputs. This is an Offline algorithm.

Al-Mamory and Zhang [4,18,19] presented an approach to make Julisch's algorithm Online and added details for selecting parameters.

In paper [20] the naïve Bayesian Classification is use for intrusion detection system. The proposed algorithm achieved high detection rate and significant reduce false positives for different types of attacks.

In paper [21] author propose an anomaly detection method using "k-Means +C4.5", a method to cascade k-Means clustering and the C4.5 decision tree methods for classifying anomalous and normal activities in a computer network.

In paper [22] propose a hybrid intrusion detection system that combines k-Means and two classifiers: K-nearest neighbor and Naïve Bayes for anomaly detection. This system can detect the intrusions and further classify them into four categories.

In paper [23] a hidden Markov method based alert prediction framework is proposed. Alert clustering is employed to group selected alert attributes together. Source IP address, destination IP Address and alert type are used.

In paper [24] IDS alerts are clustered and false positive alerts are removed with artificial neural network.

3 TABLES AND FIGURES

In this section, we introduce 3-layer architecture to improve the correlation system. Architecture of the proposed method is shown in Figure 1.

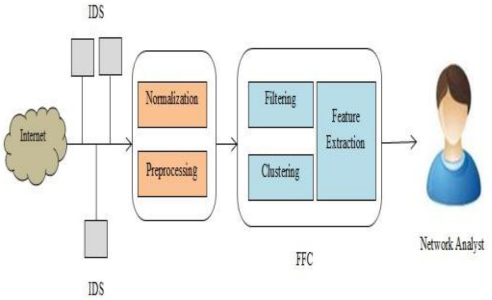
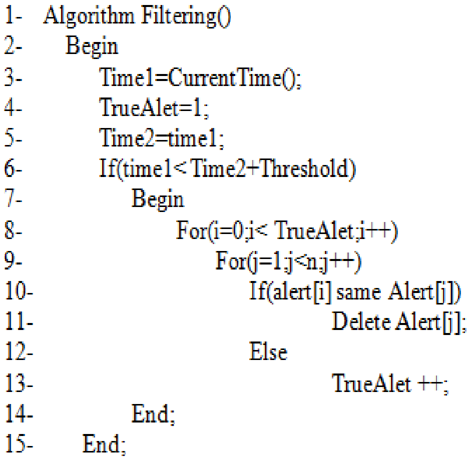


Fig. 1. architecture of the proposed method

According to the Figure1, it is shown that Intrusion Detection Systems do preprocessing and normalization on alerts that receive from the Internet. Normalization and preprocessing are converting alerts' format in different IDS to a general format. Thence, alerts are given to the FFC algorithm. This algorithm has three steps. In the first step, iterative alerts are filtered and removed. In the second step, alerts' features are expanded to increase accuracy of clustering algorithm which is third step. Each of these steps is described below.

3.1 Filtering

Filtering is essential for deleting of similar and iterative alerts. For filtering, incoming alerts are periodically checked over a period which is determined with a threshold and similar alerts are removed. The following algorithm shows this work.



```
Algorithm Filtering()
  Begin
      Time1=CurrentTime();
      TrueAlet=1;
      Time2=time1;
      If(time1<Time2+Threshold)
          Begin
              For(i=0;i< TrueAlet;i++)
                  For(j=1;j<n;j++)
                      If(alert[i] same Alert[j])
                          Delete Alert[j];
                      Else
                          TrueAlet ++;
          End;
    End;
```

Fig. 2. Filtering Algorithm

Filtering is essential for deleting of similar and iterative alerts. For filtering, incoming alerts are periodically checked over a period which is determined with a threshold and similar alerts are removed. The following algorithm shows this work.

For each alert that is entered to the system, it is checked with the previous alerts. If it is similar with each of the previous alerts, it will be removed. Otherwise, it will be added as a separate alert to different alerts' set. Of course we know that, many of the same attacks are done from different origin IPs to different destination IP that will not be removed with this algorithm because of different IPs. To improve this work, IPs' class is used instead of IPs themselves. For example, 168.1.10.11 is known as B class.

3.2 Feature Extraction

In this section, we define semantic expansion of alerts by combining the features of intrusion detection systems with features that can be gained from an attack. Alerts which are produced by intrusion detection systems have low semantic level. These alerts typically include basic information such as port number and IP address. However, there is a lot of background knowledge, which represents the relationship between the various components of a computer attack and the investigated network structure. Our idea is that, more accurate and appropriate clustering can be done on alerts with semantic expansion of alerts' information that means considering such information. We should consider an attack with all of its features to be able to extract new features for alerts. We show an attack as a tree that can be seen in Figure 3.

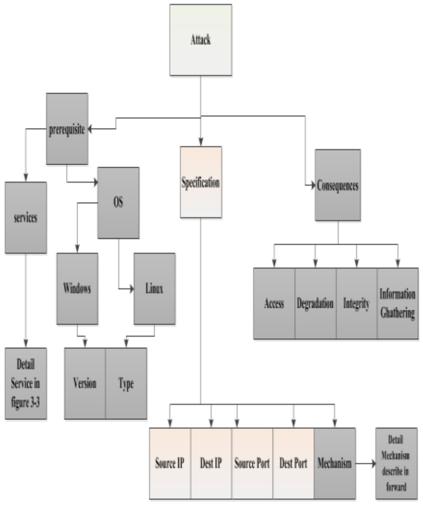


Fig. 3. attack tree

Detailed features have not been shown in Figure 3 and will be shown completely in parts of each section. Gray colored areas show the information that we add to alerts' information. So, we will be able to reduce volume of alert. According to Figure 2, we realize that an attack is composed of three parts. The first part is prerequisite of an attack that has two parts. Its two parts are operating system and service. Prerequisite means conditions that victim's system should have them. It means that in order to an attack be done successfully, operating system and desired service of this attack should be available in the victim's system. Services are resources or software available on systems inside the network that have holes and attacker use them to login victim's system. Figure 4 shows the features used for the service.

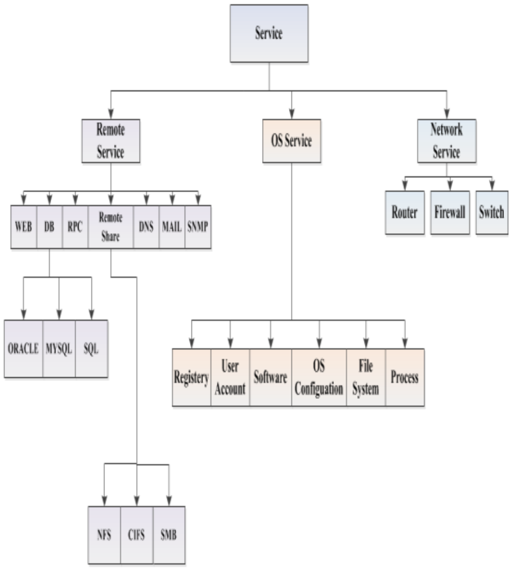


Fig. 4. features used for services

It should be noted that some alerts of intrusion detection system may require more than one service. In this case, we put these services next together. For example, attacks that can be performed against the database require a Web service in addition to the database service that will be shown as DB, WEB. In this case, in table of services for each service a column is assigned and DB service is written in column 1 and WEB service is written in column 2. Second part belongs to specification of an attack that the most basic information of an attack is there. Attack mechanism shows the method used for a special attack. For example, SQL Injection is a mechanism for database type attacks. Complete information about the mechanism is: Data Manipulation, Cross-site Scripting, Backdoor, Rootkit, Trojan, Buffer Overflow, Replay Attack, SQL Injection, Remote Execution, Port Sweep, Worm, Virus, Spyware, Application Exploit, Script Injection and Port Scan. May be used more than one mechanism for an alert. In this case, we put these mechanisms next together and allocate each mechanism a column in mechanisms' table. The third section added to the alerts of intrusion detection systems is consequence of an attack which shows the result of an attack on victim's system or a server. If prerequisite of an attack and its properties are done successfully, consequence will be produced on victim's system by the attack. Consequences can be one of the following types.

- **Access:** This feature shows that intruder has been able to access his desired system which has the following features: Server Access, User Account Access or Resource Access.
- **Degradation:** This feature shows that intruder has done degradation attack on his desired system.
- **Integrity:** This feature shows that intruder has changed sent or received information of desired system and has eliminated their accuracy.
- **Information Gathering:** This feature shows that intruder is collecting information from victim's system.

Expanded alerts are achieved by combining this information with information produced by intrusion detection systems and analyst can use them. In fact, semantic expanded of alert's information means adding prerequisite, mechanism and consequence of attacks to alerts generated by intrusion detection systems. Alert's basic information is used to create expanded alert. This information is stored in a table called TableBody. This table has the following features:

TableBody (alert message, source IP address, source port number, destination IP address, destination port number)

Alert message is a feature that shows type of alert for generated alert. For example, ICMP PING is a message that indicates an attack has occurred that its type is ICMP or GPL SMTP SSLv2 Server_Hello request is a message that indicates an attack has occurred that its type is SMTP. Using this feature and defined information table, new features of attack impact, attack mechanism, service and operating systems are obtained. There is limited number of attacks. With these attacks' investigation and help of resources such as CAPEC website that provide this information, new features can be defined for basic alerts. It should be noted that once at the beginning of the work with regard to existing attacks we obtain this information for all the available attacks and store them in TableExpand table. This table has the following features:

TableExpand (alert message, alert impact, mechanism 1, mechanism 2, mechanism n, service 1, service 2, service n, Operation System).

Intrusion detection systems generate thousands of alerts everyday and our purpose is creating expanded alerts. According to the Figure 4, method of creating these alerts is as follow: each alert that intrusion detection system produces the basic properties of these alerts are selected and placed in TableBody table. Other hand, alert message is searched in TableExpand table. When the search is performed, elements of these two tables do natural join and are placed in AlertTable table.

3.3 Clustering Alerts

Clustering is grouping similar samples together in a data volume. To calculate the similarities or distinctions, it is necessary to find variable type of alerts' properties. Based on this criterion, we define the similarity between them. Thus, we consider each of the properties used for expanded alerts as a variable. According to the type of variables and properties of expanded alerts, we reach the conclusion that variables are nominal. For example, expanded alerts can be defined as follows for feature of attack's impact.

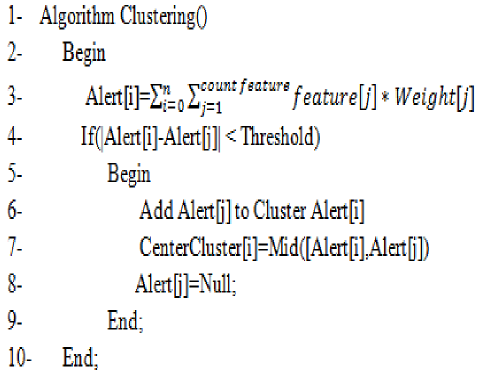
Access = 1, Degradation = 2, Integrity = 3, Reconnaissance = 4 and for other features of string do the same work. The formula 1 is used to calculate the difference between nominal variables.

$$Dissimilarity = \frac{A-K}{A},\ Similarity = 1 - Dissimilarity \qquad (1)$$

Equation1: Cluster similarity

In formula 1 A is the number of expanded alerts features and K is the number of features that have equal value between these two alerts. K-Means, KNN and Naïve Bayes have been used in [25] for alerts' clustering. In this paper, we improve K-Means to increase detection rate. It should be noted that these algorithms are done on expanded alerts. The method is as follow algorithm. We cluster expanded alerts with use of algorithm presented in Figure 5 after calculating the differences and similarities.

The process of below pseudo-code is as follows: The algorithm has two input objects. The first input is expanded alerts' table. The second input is similarity percentage that analyst determines it. It is a number between 0 and 1 that determines the degree of required similarity for clustering. The first alert put first cluster. Condition of creating new cluster is as follows: If the similarity between two alerts is less than desired similarity percentage considered as threshold, it should be placed in a new cluster because of lacking minimum required similarity. If it has minimum similarity, it should be placed in a cluster that similarity of that alert with that cluster will be more than other clusters. If there is not an appropriate amount for each feature of an alert placed in a cluster, its value will be set to UNKNOWN and that feature will not be considered in calculating clustering. That alert was given to each cluster, known as a false alert and the cluster mean is updated with the mean of its members.



```
Algorithm Clustering()
    Begin
        Alert[i]=$\sum_{i=0}^{n}\sum_{j=1}^{count\ feature} feature[j] * Weight[j]$
        If(|Alert[i]-Alert[j]| < Threshold)
            Begin
                Add Alert[j] to Cluster Alert[i]
                CenterCluster[i]=Mid([Alert[i],Alert[j])
                Alert[j]=Null;
            End;
    End;
```

Fig. 5. expanded alerts' clustering pseudo-code

On the other hand, if similarity percentage of threshold is set to zero, then all alerts will be placed in one cluster. But, if it is set to 1, then the same alerts will be placed in one cluster. Simply, if accuracy is more important for us, we will consider similarity percentage close to 1. If we need less cluster number, we will consider similarity percentage close to 0. This algorithm is similar to K-means algorithm with this difference that the number of clusters should be known at first while there is not this possibility for alerts and the number of clusters is unknown at first.

4 EQUATIONS

The data set used, includes of 5 weeks training data and 2 weeks testing data. For evaluation, the proposed algorithms are applied on the training and testing data. To evaluate the proposed method, the following factors are considered:

- Alert removal rate in the filtering step: It calculates alert count which is removed in the filtering step that is calculated from equation2.

$$\text{RAF(Removed Alert in Filtering)} = \frac{Output\ Alerts\ count}{Input\ Alerts\ count} * 100 \qquad (2)$$

Equation2: Removed alert in filtering

- The overall accuracy of the proposed system: The overall accuracy that is obtained by considering filtering and clustering steps together. It is obtained from equation3.

$$\text{Total Accuracy} = \sum_{i=0}^{cluster\ count} \frac{alerts\ cluster[i] - false\ alerts\ cluster[i]}{initial\ Alerts} * 100 \quad (3)$$

Equation3: Total accuracy

Table 1: Evaluation results of the overall alerts' detection percentage

	DARPA	IUT2012
Initial Alerts	60000	98000
RAF%	20.52	20.52
Total Accuracy for thr=0.25	74.73%	74.73%
Total Accuracy for thr=0.50	85.09	85.09
Total Accuracy for thr=0.75	96.66	96.66

The overall alerts' detection percentage has been done with regard to proposed clustering for alerts in Table 1.

4.1. *Comparison of the proposed system with similar systems*

DARPA and IUT2012 data set has been used to evaluate the proposed system with similar systems. This data sets have been used in the all similar systems. So, we use from this data sets for evaluation. Table 2 shows the results of evaluation with similar systems.

Table 2: Comparison results with similar approaches for DARPA and IUT 2012 data sets

	Total Accuracy%	False Alerts %
Julisch[3]	53	47
Almamory [4]	63.50	36.5
Amuthan[21]	99.60	10
Kunda[22]	99	40
Bakhtiari[24]	75.93	4
Proposed System for thr=0.75	96.66	3.34

In Table 2, the technique used for different algorithms has been shown in the table. Detection Ratio in the proposed approach is better than similar approaches.

5 CONCLUSION AND FUTURE WORKS

The system presented in this article fulfills several goals of a correlation system. As previously mentioned, correlation system has several goals such as reducing the volume of alerts and eliminating false positive alerts. Works that can be done for the future are as follows:

- Generating expanded alerts automatically

New features manually added and were processed manually with studding different resources in this article. Selecting these features automatically using learning machine algorithms is one of the most important strategies in the future.

6 REFERENCES

[1] S. Manganaris, M. Christensen, D. Zerkle, and K. Hermiz, "A data mining analysis of RTID alarms," Computer Networks, vol. 34, pp. 571-577, 2000.

[2] K. Julisch, "Clustering intrusion detection alarms to support root cause analysis," ACM Transactions on Information and System Security (TISSEC), vol. 6, pp. 443-471, 2003.

[3] K. Julisch, "Mining alarm clusters to improve alarm handling efficiency," in Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual, 2001, pp. 12-21.

[4] S. O. Al-Mamory and H. L. Zhang, "Intrusion detection alarms reduction using root cause analysis and clustering ", Computer Communications, Vol. 32, PP. 419-430,2/12/ 2009.

[5] S. O. Al-Mamory and H. L. Zhang, "A survey on IDS alerts processing techniques," presented at the Proceedings of the 6th WSEAS international conference on Information security and privacy, Tenerife, Spain, 2007.

[6] R. Yusof, S. R. Selamat, and S. Sahib, "Intrusion alert correlation technique analysis for heterogeneous log," IJCSNS International Journal of Computer Science and Network Security, vol. 8, pp. 132-138, 2008.

[7] A. Xinzhou. Qin, "Probabilistic-Based Framework for INFOSEC Alert Correlation", College of Computing Georgia Institute of Technology, 2005.

[8] P. Ning, D. Xu, C. G. Healey, and R. S. Amant, "Building attack scenarios through

integration of complementary alert correlation methods," in Proceedings of the 11th Annual Network and Distributed System Security Symposium, 2004.

[9] P. Ning, Y. Cui, and D. S. Reeves, "Constructing attack scenarios through correlation of intrusion alerts,"Proceedings of the 9th ACM conference on Computer and communications security, 2002, pp. 245-254.

[10] O. M. Dain and R. K. Cunningham, "Building scenarios from a heterogeneous alert stream," in Proceedings of the 2001 IEEE workshop on Information Assurance and Security, 2001.

[11] O. Dain and R. K. Cunningham, "Fusing a heterogeneous alert stream into scenarios," in Proceedings of the 2001 ACM workshop on Data Mining for Security Applications, 2001.

[12] R. Smith, N. Japkowicz, M. Dondo, and P. Mason, "Using unsupervised learning for network alert correlation," in Advances in Artificial Intelligence, ed: Springer, 2008, pp. 308-319.

[13] R. Smith, N. Japkowicz, and M. Dondo, "Clustering using an autoassociator: A case study in network event correlation," in Proceedings of the 17th IASTED International Conference on Parallel and Distributed Computing and Systems, Phoenix, AZ, 2005, pp. 613-618.

[14] N. Japkowicz and R. Smith, "Autocorrel I: A Neural Network Based Network Event Correlation Approach," DTIC Document2005.

[15] F. Valeur, G. Vigna, C. Kruegel, and R. A. Kemmerer, "Comprehensive approach to intrusion detection alert correlation," Dependable and Secure Computing, IEEE Transactions on, vol. 1, pp. 146-169, 2004.

[16] F. Valeur, "Real-Time Intrusion Detection Alert Correlation," Computer Science, University of California Santa Barbara, California, 2006.

[17] K. Julisch and M. Dacier, "Mining intrusion detection alarms for actionable knowledge," in Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining, 2002, pp. 366-375.

[18] S. O. Al-Mamory and H. Zhang, "IDS alerts correlation using grammar-based approach," Journal in computer virology, vol. 5, pp. 271-282, 2009.

[19] S. O. Al-Mamory and H. L. Zhang, "New data mining technique to enhance IDS alarms quality ", Computer Communications, 2010.

[20] J. Manish and R. Vinit, "An Improved Techniques Based on Naïve Bayesian for Attack Detection ", International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol. 2, Issue 1, 2012.

[21] P. M. Amuthan, R.Rajeswari and R. Rajarm, "Network Anomaly Detection by cascading K-Means Clustering and C4.5 Decision Tree Algorithm ", International Conference on Communication Technology and System Design , vol. 30, pp. 174–182 ,2011.

[22] H. Om and A. Kunda, "A Hybrid System for Reducing the False Alarm Rate of Anomaly Intrusion Detection System ", Recent Advances in Information Technology (RAIT), 2012 1st International Conference IEEE , pp.131 – 136, 2012.

[23] Udaya Sampath K. Perera Miriya Thanthrige and j. Samarabandu and x.wang, "Intrusion Alert Prediction Using a Hidden Markov Model ", eprint arXiv:1610.07276 ,2016.

[24] F.Ch. Bakhtiari and m. K. Mirnia, " evaluating artifcial neural network in ids alert management ", journal of scientificresearch and development2 , pp.316 – 319, 2015.