Performance of an Intrusion Detection System under Different Techniques

Sadeq AlHamouz
Department of Computer Information Systems
Middle East University
Amman, Jordan
shamouz@meu.edu.jo

***Abstract*— Nowadays, with the rapid growth in technologies, which depend on computers systems and networks, threats are also increasing enormously. So, a huge number of approaches have been developed to protect systems and networks and to increase the security since it is an essential requirement in the majority of the applications. In this paper, a statistical Naïve Bayesian method is applied in an IDS system using different scenarios. The performance of the IDS is measured through experiments using NSL-KDD dataset.**

Keywords– Intrusion Detection System, Attack trends, Security, Attacker, Techniques, Network threats, Network defense.

I. INTRODUCTION

Previously, several researchers have described the design of IDSs to offer details and descriptions of the main characteristics of those systems that are applicable and relevant in the detection of attacks. The design of IDSs depends on the experiences, which are resulted from the improvement and use of those systems in various fields and on the analysis of several types of attacks [1].

Some of IDS characteristics are: information, which used in the analysis, the level of the interpretation and verification of protocols and methods used in discovering activities that may signify attacks. Those systems range from simple to complex ones and differ in their characteristics [2].

In [1], a model of IDS that consists of sensors and detectors was described. The used sensors to signify the e-box of the Common Intrusion Detection Framework Architecture (CIDFA) and to recover information from a data source were described in [6]. This recovered information is inserted then to the detector. Researchers explored that the detector is a combination of both the a-box and d-box.

The IDS characteristics can be represented using two relatively simple parameters. The first parameter indicates a general characteristic of the system, such as the capability to concern accepted expression matching on information. However, this parameter has not the ability to identify the scope where it is obtainable. In other words, it cannot discover the type of information expression matching that should be concerned. The second parameter has the ability to discover the IDS scope, which determines the validity of the system characteristics [5].

The IDS scope, which is an iterative method that consists of three high-level scopes, is explored. Those scopes are: networking, user and host. Both networking and host are divided into several low-level scopes, like application layer and process, while the user scope is the human who uses the IDS [5]. Several works about the analysis of IDSs were published in order to detect attacks. Those works classify the IDSs, ID and attacks. One of those works is the MAFTIA project that uses several concepts, models and terminologies that derived from reliable fields [7, 8].

Network threats can be persons, events or objects, which can cause damages in a network. Threats also can be accidental, such as errors in calculations or malicious, such as data intended modification. Network security threats are divided into two main types; internal and external threats. The internal threats happen by a person who has a pre-defined access to the network. This access can be an account or physical access. On the other hand, the external threats happen by persons who have no pre-defined accesses to the network. Those threats are resulted from the internet or access servers [13, 14].

There are several types of attack trends, such as: threat activity trends, vulnerability trends, malicious code trends, fraud activity trends and phishing activity trends. Vulnerability is the weakness in a network that allows attacker to cooperate the accessibility and integrity of this network. Malicious code is a wide group of software threats that attack networks and systems. The most complicated threats types are obtainable by the malicious code, which uses vulnerabilities in networks. Any code that changes, obliterates or takes data permits illegal access, damages a network and/or results in several thins unrelated for users [15].

Phishing represents data from persons, groups or organizations with the use of a specific brand. Phishing attackers get several sensitive personal data of users. They need fatalities in order to offer their main qualifications. Fraud is the unauthorized or illegal use by attackers of some data that are related to a specified person [16].

Network defence is the actions taken to monitor, protect, analyse, detect, and respond to unauthorized activities in information systems and computer networks. Several systems are used in the defence of networks against attacks. The first method of protection is the IDS. IDSs have the ability to detect several types of attacks by monitoring networks. Another protection method is the firewall, which is one of the most used defence devices that range from personnel firewall to array ones. Firewalls are utilized in the protection of large networks in large organizations. They are utilized to distinguish between networks via utilizing several rules in

order to decide the allowable connections. Another protection method is the encryption, which is used to hide data using a secret algorithm. Those data are then decrypted only by a pre-defined secret key. In this way, attackers cannot reach these data. Another defence method is the authentication, which is similar to the encryption one. In this technique, messages are sent between a client and network access router by a protocol as a carrier in an authenticated way where attackers cannot reach those messages. After the authentication process, the client is defined as a Media Access Control (MAC) address that can access the network and an Access Point (AP), which is defined also as a MAC address with the same client [17, 18].

The last defence method is the physical security, which assists in the evaluation and understanding of several risks which in turn facilitates taking corrective actions. It is the physical protection level that surrounds the neighbouring the intended coverage region with the proposed level of security as well as threat model [25].

General introduction of intrusion detection systems is discussed, in section II offers an overview of IDSs. Section III discusses the IDS classification and filtering. Section IV analyses the system model of IDS using Naïve technique, the evaluation and the comparison between the proposed systems section with different features are presented in section V and conclusion is given in section VI.

II. BACKGROUND

IDSs are divided into two groups; Network IDS (NIDS) and Host IDS (HIDS). The NIDS monitors the behaviour of the system, while the HIDS monitors the calls of the system. For the NIDS, the activities of the network are independent on several ports. Random projection sketches are used in order to decrease the dimensionality of information with the use of multi-resolution non Gaussian marginal distribution in order to find out the abnormalities across several levels of aggregation [19, 20]. The entropy based method was used in the whole network traffic [21]. Both the statistical tests and the subspace techniques, which suppose that the connection features are normally distributed, were used [22, 27].

NIDS are widely used as the last defence line in order to allow several event responses when the intrusion avoidance mechanisms are not effective. This system compares the network traffic with a known database in order to detect the unwanted traffics. The main benefits of NIDS are: its ease use and few numbers of generated false alarms. In contrast, NIDS cannot detect all types of attacks in an effective way. Some of those attacks are: U2R, R2L [13].

The most common types of attacks are: DOS, U2R, R2L and probe attacks: [11]

Denial of service (DoS) attackers use obtainable or unobtainable memory sources in order to control requirements or to ignore rights of users from service, some of those attackers are SYN flood, neptune, back, smurf, land and teardrop.

User to Root (U2R) attackers use an account of a system user in order to realize root access to the required system as the user privilege (e.g. buffer overflow)

Remote to Local (R2L) attackers send several packets to the system without having an account on this system (e.g. password guessing).

Probe attackers find out information or recognized threats. Attackers can easily make an attack with the use of this information (e.g. ping sweep, port scan)

The HIDS works on discovering the system calls. Those works are divided into two groups; sequence based works and feature based works. The sequence based works depend on the events chronological orders, while the second works consider the calls as independent information elements. In [12], information was simplified by creating a database storing calls subsequence and then examined them. In [14], the richer group of attributes was assumed to be a return value where influences are related to the system calls.

HIDS is used in the detection of intrusions via examining several computing activities models, like the CPU usage and memory. HIDS analyses the system settings, system calls, local log inspections and more. It is used widely due to its effectiveness in the detection of known attacks. On the other hand, this system is not effective in the detection of new attacks [10].

Both NIDS and HIDS differ from each other, but in the same time, both are complement to each other. In other words, a real secured environment needs the use of both systems in order to offer a forceful system that is considered as the foundation for monitoring and detecting misuses. This combination can filter alerts as well as notifications in a perfect way, which in turn helps in controlling and reacting to misuses.

The main three types of detection methodologies are: Pattern matching, protocol analysis and anomaly detection.

The pattern matching methodology is used to determine how frequently an applicant pattern happens and also to determine some data about its frequency distribution throughout a text. Pattern is set of strings, in which each string is a series of symbols. The best pattern has a small number of strings. This technique depends on finding out how many times a string is occurred in a text and determining its incident positions [9].

The protocol analysis technique is used to discover the locations as well as lengths of fields that exist in the protocol packets. The structure of both needs and responses can be understood by these packets with the use of reverse engineering. This technique is carried out via hand using perception as well as a protocol analyser instrument, like tcpdump. It can be used in the NIDSs in order to find out the higher level semantic framework from a traffic set [3, 11].

The anomaly detection technique is used in order to discover patterns in data, which are not matched with the prospected behaviour. Those patterns can be anomalies, exceptions, contaminants, peculiarities or outliers. The most used patterns in this technique are the anomalies and outliers. This technique can discover wide applications use, like fraud detection of credit cards and intrusion detection. The most important point of this technique is that anomalies that exist in data are converted into important data in several applications [21, 26].

III. Multi-Layer Bayesian Filtering Technique

Multi-layer Bayesian filtering technique is used in the IDSs with the use of KDD dataset. KDD is one of the main practical and realistic sets that contain actual attacks. It is used in the modelling and evaluation of IDS and it assists in the comparison between experimental results. The model of Bayesian IDS identifies features, which have diverse happening probabilities in both attacks and TCP traffic. Initially, Bayesian filter is qualified by a pre-classified traffic and then it corrects the features probabilities. After that, it calculates each TCP probability and categorizes it as a normal traffic or attack one. Bayesian filter contains two component; training engine and testing engine. The training engine calculates the numbers of both good and bad records, then it creates three hash tables; two of them contain the frequency of both good records attributes and bad records attributes and the third one contains those attributes and their scores. [15, 25].

The testing engine is used to test the resultant training engine using the KDD dataset and to determine if the record is an attack or not based on a specified threshold. Accuracy and results of tests depend on databases, features and threshold value. The following percentage expressions are used in the analysis of data: [16, 13, and 24].

True Negative (TN): normal records which are correctly classified, True Positive (TP): attack records which are correctly classified, False Positive (FP): normal records which are incorrectly classified as attacks and False Negative (FN): attack records which are incorrectly classified as normal. By using these expressions, both the detection rate and classification rate can be represented as follows:

$$\text{Detection Rate (DR)} = \frac{\text{TP}}{\text{TP} + \text{FN}} \qquad (1)$$

$$\text{Classification Rate (CR)} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FPFN}} \qquad (2)$$

Three improved Bayesian filters are explained and compared with each other in order to determine the most accurate filter in the detection of attack records.

- Improved Bayesian Filter 1 (IBF1)

IBF1 is a one-layer filter. In this filter, the normal records are filtered again for several times with the use of engines that have different settings of threshold and features, where the output normal records of one engine are the inputs of the next engine. This process enhances the accuracy, where attack records of all engines are collected. Figure 1 shows the IBF1 model [18, 23].

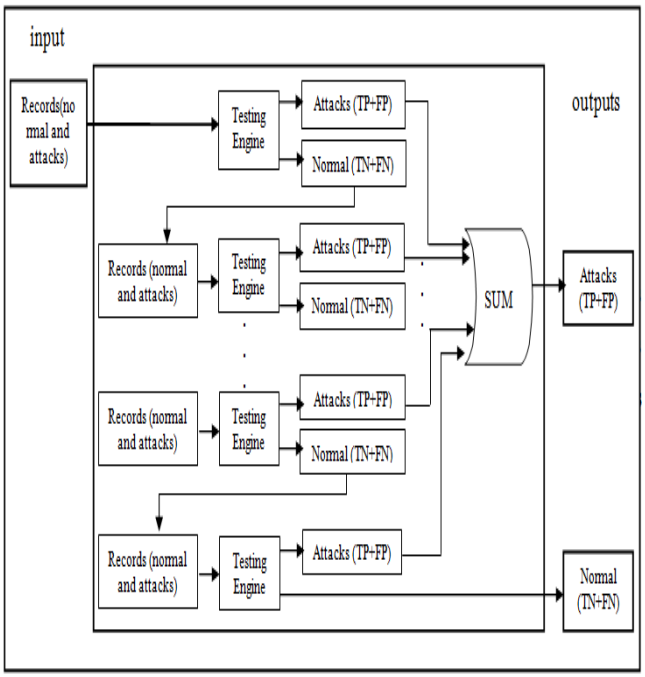

Fig. 1 IBF1 model

- Improved Bayesian Filter 2 (IBF2)

IBF2 is a one-layer filter. In this filter, the normal records are filtered again for several times with the use of engines that have different settings of databases, where the output normal records of one engine are the inputs of the next engine. This process enhances the detection rate but it has high FP percentage which is a problem. Figure 2 below shows the IBF2 model [17].

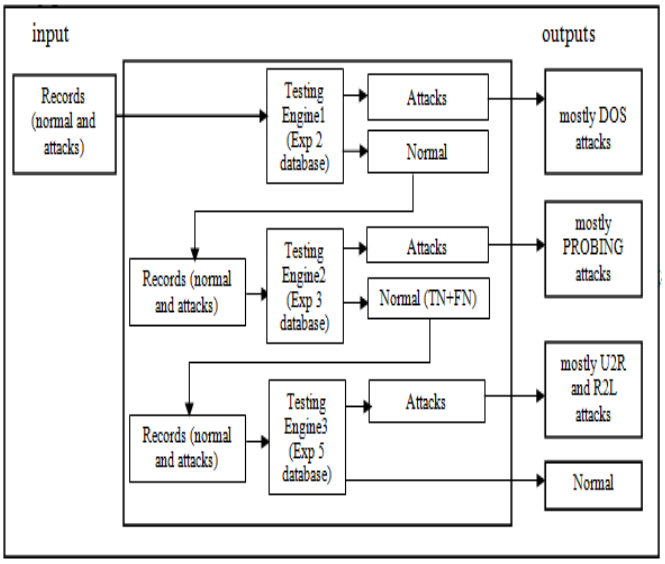

Fig. 2 IBF2 model

- Improved Bayesian Filter 3 (IBF3)

IBF3 filter consists of two layers in series. In the first layer, attack records are filtered again, while in the second layer, both attack and normal records are filtered. This combination gives the highest detection rate that equals to 96.85% since both types of records are filtered again. Figure 3 below shows the IBF3 model [19, 22].

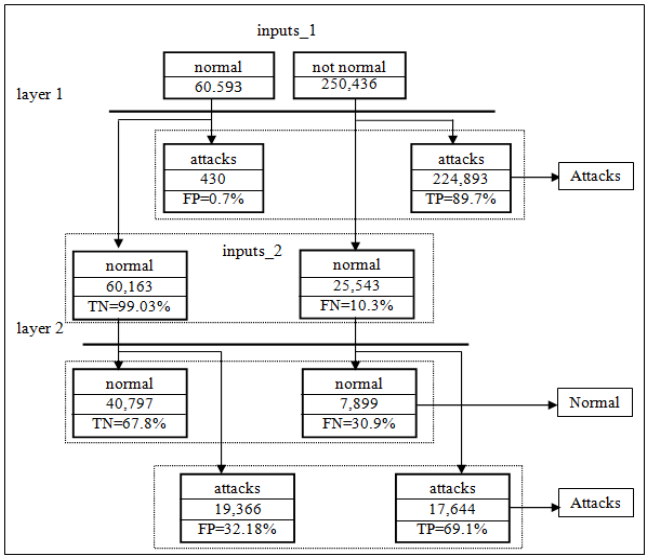

Fig. 3 IBF3 model

IV. SYSTEM MODEL

In this paper, a Naïve Bayesian based IDS is explored and discussed. Initially, this section offers a brief description concerning the Naïve Bayesian technique with exploring their principles of work and main equations. After that, those systems are trained and tested using the NSL-KDD database in order to measure and evaluate their performance. This database composed of 41 network connection features, where the names of those features are demonstrated in this section. The NSL-KDD database is applied in this work using two sets of features numbers for both classification methods; (5,10,24,29,33,34,38,40) and (2,5,8,23,30,34,35,38). The proposed classification methods are applied on the proposed IDSs using those sets of features.

The Naive Bayes algorithm is applied on the IDS to find the probability of the presence of an attack in a computer network. When the computed attack probability is high but not enough to be considered as attack, then the computer network produces a report and warns the administrator of the system. The Naive Bayes can be used to classify any unknown object when the network is quantified based on its attributes values by using the following expression equation (3): [20]

$$P(C_j/X) = \frac{P(X/C_j)\,P(C_j)}{P(X)}$$

$$P(C_j/X) > P(C_i/X), 1 \le i \le m, i \ne j \qquad (3)$$

Where: C_j class that belong to group of m classes C1, C2…Cm, X represents the data sample which not known and P(X) is constant for each category. The proposed IDSs use Naive Bayes Eq. (3) to classify network connections as normal or attack based on their features. In the proposed IDS the NSL-KDD data set is used for training and testing stages to evaluation. NSL-KDD data sets include 41 features of the network connection.

V. SIMULATION AND NUMERICAL RESULTS

In this section, the obtained results for developed Naïve Bayes based Intrusion Detection Systems (IDSs) using the proposed sets of features in references [28] and [29] are presented. The NSL-KDD database is used to measure the performance of both systems, where those systems differ in the used set of features. All the simulation results are obtained using the MATLAB program.

The following figure shows the obtained results of the proposed Naïve Bayes based IDS using the proposed set of features in [28] for the first case.

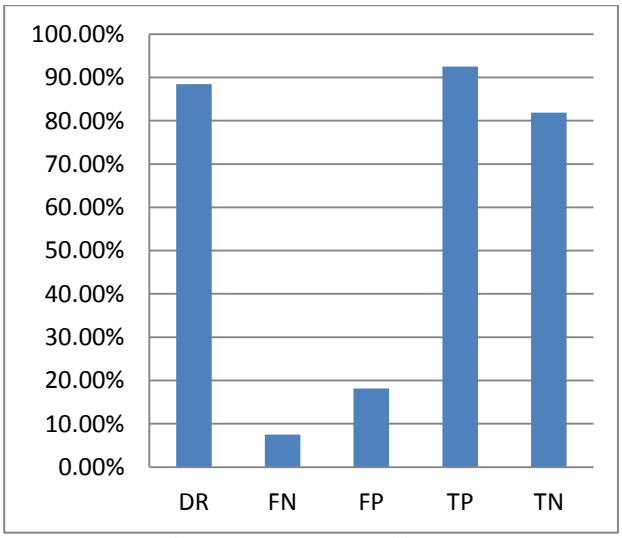

Fig. 4 Results of using the proposed set of features in [28] in Naïve Bayes

As shown in the figure above, the system has DR 88.51% and obvious FN and FP rates, where the resultant FN rate in 7.49 % and FP rate is 18.16%. Thus, this system needs further enhancements based on eliminating all records that result in false alarms.

The obtained results of the proposed Naïve Bayes based IDS in [29] for the first case; all records are shown in the following figure.

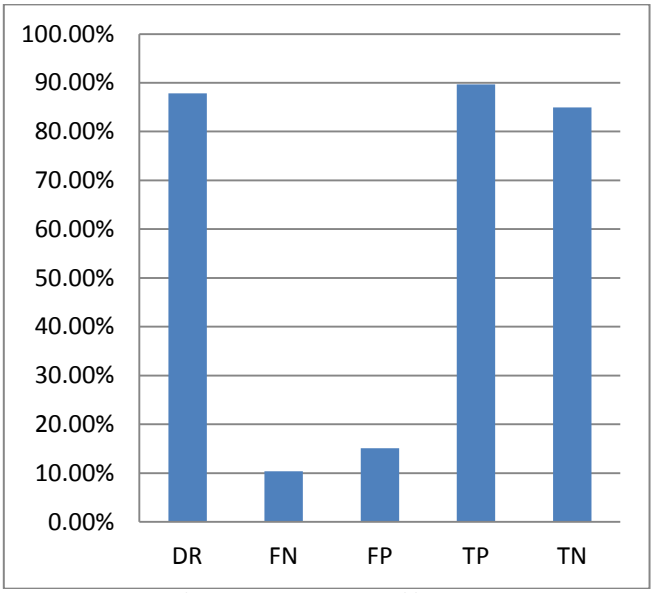

Fig. 5 Results of using the proposed set of features in [29] Naïve Bayes

As shown in the figure above, the application of the proposed Naïve Bayes based IDS on the second set of features for all records results in DR=87.2%, 10.38% FN rate and 15.11% FP rate.

VI. Concluding Remarks

This paper proposed the development of advanced Intrusion Detection System (IDS) using Naïve Bayesian classifier to decrease the number of generated false alarms: false positives and false negatives, improve the network security and enhance the detection rate of several types of attacks. Naive Bayesian method was applied on the constructed IDS in different scenarios using the MATLAB program, where then a comparative study among them was conducted based on analyzing the performance parameters and determining the most efficient statistical method in detecting various types of attacks. The NSL-KDD database was used to measure the performance of the implemented systems, where it composed of 41 features of the network connection.

For the Naïve Bayesian classifier, two systems have been implemented and analyze. Using the proposed features numbers in [28] and [29], the obtained DRs are 88.51% and 87.2%, FP rates are 18.16% and 15.11% and FN rates are 7.49% and 10.38%, respectively.

References

[1] M., Dacier and D., Alessandri, ‘’ VulDa: A Vulnerability Database’’, 1999

[2] D., Alessandri, ‘’ Attack-Class-Based Analysis of Intrusion Detection Systems*’’*, a thesis submitted to School of Computing Science, University of Newcastle upon Tyne, 2004

[3] P., Pporras, D., Schnacenberg, S.S., Chen, M., Stillman and F., Wu, ‘’ The Common Intrusion Detection Framework Architecture’’

[4] MAFTIA Consortium, ‘’ Architecture and revised model of MAFTIA’’, R. Stroud, ed. Malicious- and Accidental- Fault Tolerance for Internet Applications, 2001

[5] MAFTIA Consortium,’’ Towards a Taxonomy of Intrusion Detection Systems and Attacks’’, D. Alessandri, ed. Malicious- and Accidental-Fault Tolerance for Internet Applications

[6] J., Xu and C.R., Shelton, “Intrusion detection using continuous time Bayesian networks”, *Journal of Artificial Intelligence Research*, vol. 39, no. 1, 2010

[7] G., Dewaele, K., Fukuda and P., Borgnat, ‘’ Extracting hidden anomalies using sketch and non-Gaussian multi-resolution statistical detection procedures’’, *proceedings of the 2007 workshop on Large scale attack defenc*e, pp. 145-152, 2007

[8] A., Lakhina, M., Crovella and C., Diot, ‘’ Mining anomalies using traffic feature distributions’’, *ACM SIGCOMM Computer Communication Review - Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications*, vol. 35, no. 4, pp 217-228, 2005

[9] N., Ye, S.M, Emran, Q., Chen and S., Vilbert, ‘’ Multivariate statistical analysis of audit trails for host-based intrusion detection’’, *Transactions of Computers*, vol. 51, no. 7, pp 810–820, 2002

[10] G., Tandon, and P.K., Chan, “Modelling Multiple Time Series for Anomaly Detection”, *In the Florida Artificial Intelligence Research Society Conference*, pp 405 410, 2005

[11] A., Hofmeyr, S. ,Forrest and A., Somayaji, ‘’ Intrusion detection using sequences of system calls’’. *Journal of Computer Security*, vol. 6, pp 151–180, 1998

[12] J., Leung, ‘’ Vulnerability Management – A Guide to Managing Internal and External Threats’’, 2008

[13] Federal Information Processing Standards Publication 191 (FIPS PUB 191), ‘’ Guideline for the Analysis Local Area Network Security’’, 1994

[14] M., Heidari, Malicious code in depth, pp 1-21, 2004

[15] Financial Crimes Enforcement Network (FCEN), ‘’Mortgage Loan Fraud’’, 2008

[16] B., Raman, Cryptography and Network Security, Department of CSE, IIT Kanpur2005

[17] D., Faria, Scalable Location-Based Security in Wireless Networks khan, A Dissertation Submitted To The Department Of Computer Science And The Committee On Graduate Studies Of Stanford University In Partial Fulfillment Of The Requirements For The Degree Of Doctor Of Philosophy, 2006

[18] P., Gogoi, D.K., Bhattacharyya,B., Borah and J. k., Kalita, "MLH-IDS: A Multi-Level Hybrid Intrusion Detection Method", *The Computer Journal Advance Access published May 12*, vol. 58, no. 4, 2013.

[19] J., Hu, ‘’ Host-Based Anomaly Intrusion Detection’’, *Springer*, pp 235-255, 2010

[20] G. Navarro, ‘’ Pattern Matching’’, pp 1-24

[21] M.A., Beddoe, ‘’Network Protocol Analysis using Bioinformatics Algorithms’’, *Proceedings of the Seventh International Network Conference*, 2005

[22] H., Dreger, A., Felmann, M., Mai, V., Paxson and R., Sommer, ‘’ Dynamic Application-Layer Protocol Analysis for Network Intrusion Detection’’, *USENIX-SS'06 Proceedings of the 15th conference on USENIX Security Symposium*, vol. 15, no. 18, 2006

[23] V. Chandola, and V. Kumar, ‘’Anomaly Detection : A Survey’’, *ACM Computing Surveys (CSUR)*, vol. 41, no. 3, pp 1-72, 2009

[24] H. Altwajry and S. Algarny, ‘’ Multi-Layer Bayesian Based Intrusion Detection System’’ *Proceedings of the World Congress on Engineering and Computer Science*, vol. II, 2011

[25] U. Aickelin, J. Twycross and T.H. Roberts, ‘’Rule Generalization in Intrusion Detection Systems Using SNORT’’, *International Journal of Electronic Security and Digital Forensics*, vol. 1, no. 1, pp 101- 116, 2007

[26] Z., Sun, R., Kaucic, P., Mendoca, and A., Can, ‘’ A Statistical Approach to Industrial Anomaly Detection’’, pp 1-9, 2007

[27] D.C. Montgomery, ‘’ *Introduction to Statistical Quality Control*’’, 4th edn, Wiley, New York, NY, 2001

[28] W., Al-Sharafat and R., Naoum," Significant of Features Selection for Detecting Network Intrusions " , *International Conference for Internet Technology and Secured Transactions ICITST*, 2009

[29] P., Bhoria and K., Garg,” Determining feature set of DOS attacks”, *international Journal of Advanced Research in Computer Science and Software Engineering* , Vol. 3, Issue 5, May 2013