International Journal of Grid and Distributed Computing
Vol. 10, No. 2 (2017), pp.51-62
http://dx.doi.org/10.14257/ijgdc.2017.10.2.05

Hybrid Network Intrusion Detection System Using Machine Learning Classification and Rule Based Learning System

Urooj Aslam, Ezzat Batool, S. Nadeem Ahsan and Abdullah Sultan

Faculty of Engineering, Science and Technology, Main Campus, Iqra University, Defence View, Shaheed-e-Millat Road (Ext.) Karachi-75500, Pakistan
uroojaslam14@gmail.com, ezzat786@hotmail.com, dr.ahsan@iqra.edu.pk, abdullah.sultan1994@gmail.com

Abstract

One of the greatest challenges of today's rule-based network intrusion detection system (NIDS) is the largest value of its false positive rate which makes rule-based NIDS system unreliable. To avoid large values of false positive rate, a hybrid system based on multiple intrusion detectors in series has been proposed in this research paper. The proposed system uses a rule-based learning and machine learning classification to automatically detect attacks more precisely against computer networks and systems automatically. Our approach uses two different learning styles in series to detect network intrusions. First, we use a rule-based system to identify incoming network packets as an intrusion or normal packets, and then use trained model of machine learning classifier to further validate whether the incoming packets are intruding or normal packets. For the rule-based system, we use "SNORT" and for machine learning classification we use simple logistic, J48 and Sequential Minimal Optimization (SMO). The final decision about intrusions is based on the prediction of both the learning systems, we use "OR" gate logic on the output of both the detectors to identify attack more precisely. Our experimental results show that our approach can successfully reduce the false positive and false negative rate of rule-based NIDS.

Keywords: *Network intrusion detection, Snort, machine learning, simple logistics, SMO*

1. Introduction

In recent years, the usage of internet is growing every day, which increases the violation of security, more and more businesses are putting their sensitive data on the web for availability purpose. Therefore, a secured infrastructure must develop to protect the information from the malicious users. However, firewall and antivirus and other access control schemes are present, but they are not enough. Thus, a security plan has been emerging in for the past few years called "Intrusion Detection System." It is used to strengthen the security system like any other security tools. IDS could be hardware or software or a combination of both [19].

Network-based IDS monitor traffic on a network segment of the subnet by placing NIC in promiscuous mode to collect the entire traffic passing through the subnet. It reads the packets and matches them to the library of known attacks if the attack is identified, then NIDS report the administrator of suspicious threat. NIDS is typically placed on the network where the firewall is installed to see if someone tries to break through the firewall. There are two types of NIDS according to the system interactivity; On-line and Off-line NIDS. Off-line NIDS deals with stored data while On-line deals with real-time traffic analysis which is mainly the goal of this paper, it scans network packets and matches them with some rules to detect an attack [13].

ISSN: 2005-4262 IJGDC

Because of the increase in the diversity of attacks and new attacks are developing every day one should provide the system with flexibility and adaptation. Although Anomaly-based network intrusion detection can detect novel attacks even before they have been studied by security analyst and signature/rule-based network intrusion detection system is good at detecting specified and known attacks. Two approaches together make a system in identifying any intrusive behavior. Machine Learning based NIDS uses anomaly-based approach and Rule-Based uses signature-based approach. Rule-based learning is used to classify packets as normal and abnormal and ML based system reduces the rate of false positive and false negative for network intrusion detection system [8]. ML can learn without being explicitly programmed, it usually starts with some knowledge, so that it can analyze, interpret and test the knowledge it has. Similarly, rule-based NIDS could identify known attacks.

Therefore, the hybrid approach makes sure no packets with intrusion passes through and enters our system. In this paper, we introduced a hybrid network intrusion detection system based on rule-based learning system and Machine Learning classification. Rule-based NIDS is used to capture real-time data by using the tool "SNORT" (open source software). Machine Learning based NIDS is used to solve the classification problem and label them as "normal" and "abnormal". To build machine learning model, we used KDD dataset [12].

According to our research hypothesis, trained machine learning model can be applied to SNORT classification data to further verify an attack identified by SNORT in real time. In order to validate our hypothesis; we used both an anomaly and signature-based techniques to classify the network traffic as "normal" and "abnormal". Our approach can be divided into two parts; In the first part "SNORT" (an IDS itself) is configured to capture network traffic in real time, and on the basis of some pre-defined rules, SNORT classified incoming network traffic as normal or abnormal (attack) traffic. After SNORT classification, we stored this information into a database. In the second part, a machine learning model is trained using KDD dataset. After model training, we used the model for the validation of SNORT classification results. The final prediction of our proposed hybrid system is based on the results of both the systems i.e., SNORT and machine learning. The classification results of snort and ML are compared, if one of the two systems declares a packet as anomaly/attack; it will be labeled an attack, which is according to OR gate logic and also fulfill the requirements of defence in depth.

This paper has been arranged as follows: In Section **II**, related work is discussed. In Section **III**, background theory is described. In Section **IV** approach and experimental setup is described. In Section **V** result and discussion is described. Our research work is concluded and open areas are identified in Section **VI**.

2. Related Work

The concept of intrusion detection system was first introduced by Fred Cohen when he noted in 1987 that it is not possible to detect an intrusion in every case and the resources will grow with the amount of usage [24]. Also, Dr. Denning assisted by Peter G. Helped to develop the first model for intrusion detection; the Intrusion Detection System (IDS) was published in 1986 [1]. Her model used statistics for anomaly detection and resulted from new IDS at SRI International named the Intrusion Detection Expert System (IDES) ran on Sun workstations and could consider both user and network level data. Likewise, we used KDD dataset in our project for the training of NIDS model. IDES includes a dual approach with a rule-based Expert System to detect known types of intrusions and statistical anomaly detection component based on profiles of users, host- based systems, and target systems. Similarly, our project is also combination of two different approaches. One is Ruled based using SNORT and another is Machine learning based.

Lunt proposed adding an Artificial neural network as a third component. She said all three components could then report to a resolve the challenges of NIDS [2]. Wisdom & Sense (W&S) developed a statistic-based anomaly detector in 1989 at the Los Alamos National Laboratory [3]. W&S proposed paper based on statistical analysis for anomaly detection. In 1990 Computer Watch at AT&T Bell Labs used statistics and rules for audit data reduction and intrusion detection [4]. In our case we also used rules for the detection of clean and malicious data. The Lunt IDES combines a statistical user profile approach with the rule-based expert system. In 1992, SRI International designed and developed an IDES learn user behavior pattern over time and detected behavior that deviates from this pattern also has a rule-based component to identify known intrusions. Lunt also added artificial neural network as a third element [5].

In 1993, SRI followed IDES with next-generation detection system NIDES. In 1998, APE developed lip-cap, later named snort and since then it is the largest used IDS/IPS. In 2000, S Mukkamala presented a paper on intrusion detection using neural network and support vector machine (SVM) [6]. In our Machine learning approach, we used SVM and Simple Logistic as algorithms for the detection of an intrusion. Also, in 2009, Jesús E. Díaz- Verdejo, Gabriel Maciá-Fernández, and Enrique Vázquez proposed a paper which gives the brief description of Anomaly-based network intrusion detection techniques, systems and challenges [7]. Our approach successfully handles the challenges such as class imbalance and feature selection. In the year 2010, Gireesh Kumar proposed work on a network intrusion detection system based on machine learning in which RST (rough set theory) used to pre-process the data and reduce the dimension; the SVM model used to learn and test the data and the results then compared with PCA [8]. Likewise, we also used PCA and Attribute Selection as techniques for the reduction of the features in our KDD data.

In 2007, Hwang et al. [18] proposed a hybrid system that combines an anomaly detection system with signature-based IDS in a cascade structure. They developed a weighted signature generation scheme to integrate Anomaly Detection System (ADS) with SNORT by extracting signatures from anomalies detected. Their proposed Hybrid IDS extracts signatures from the output of ADS and adds them into the SNORT signature database for fast and accurate intrusion detection [17].

In 2009, Gomez et al. extended SNORT by adding an anomaly detection preprocessor. They claimed that their obtained results confirmed that the database or the number of elements used to model the normal network behavior affect considerably the performance of the IDS. They verified that when the number of elements increases NIDS has less sensitivity and therefore detect few attacks. Results also denote the importance of training the system during a long time to reduce the number of false alarms.

In 2010, Robin Sommer and Vern Paxson, adopted an anomaly based approach for machine learning in outside the closed world on using machine learning for network intrusion detection. They examined the surprising imbalance between the extensive amount of research on machine learning-based anomaly detection pursued in the academic intrusion detection community, versus the lack of operational deployments of such systems. They identified several challenges which are related to machine learning based NIDS. To overcome these challenges, they also provided a guideline [20]. In 2012, AS Aneetha, TS Indhu, S Bose implemented hybrid network intrusion detection system using an expert system approach which uses real-time network monitoring with appropriate clustering techniques [9].

In In 2012 Shah, Sagar N and Singh, Ms Purnima publishes a paper on signature-based network intrusion detection using Snort and WINPCAP [21]. In 2013, K Satpute, S Agarwal, J Agarwal, S Sharma proposed a paper on Anomaly detection in NIDS using particle swarm optimization based machine learning techniques in which Particle Swarm Optimization and variants combined with various Machine Learning techniques for Anomaly detection [10].

In 2015, Zakir Malek with Dr. Bhutan Trivedi introduced a Rule Based Intrusion Detection Model using User Behavior [11]. In 2016, Özge Cepheli et al. proposed a parallel detection methodology to model hybrid intrusion detection system to accurately detect distributed DOS attacks, also known as DDoS attacks. They used both anomaly-based and signature-based detection methods in parallel [22].

Most of the related works are based on signature based NIDS system [1], [2], [4], [5]. However, there are some research work which are based on both signature and anomaly based NIDS [17], [18], [22]. Our proposed work is also based on hybrid system, i.e., we proposed to use both signatures and anomaly based NIDS.

3. Background

In this section, we will elaborate those techniques and tools which have been used to design the architecture of our proposed system.

3.1 Network Intrusion Detection System (NIDS)

Network IDS monitor network traffic for malicious activity and report to the administrator, if any violation of security occurs. Depending on the source information about IDS, it could be either network based or host based. In host-based IDS the network activity analyses are system calls or process identifier, mostly related to the OS. Network-based IDS uses traffic rate, the number of the packet, connection rate, etc. [15] Also, IDS could be signature based and anomaly based. The signature based system uses a defined pattern (signature) to analyses network activity while anomaly based trained the system with normal behavior and report when the deviation between prepared data and observed data occur [21].

3.2 Snort (Open Source Software for NIDS).

SNORT is an open-source IDS with a capability of real time traffic analysis and packet logging on IP network, with additional capabilities. Snort is a full-fledged open source network intrusion detection system (NIDS). Snort can perform protocol analysis and content searching/matching and utilizing predefined signature. Snort can be used as lightweight intrusion detection system [13]. It is a Rule-Based system which uses specific rules for the detection of known attacks. Snort supports a simple rule language that matches against network packets, generating alerts or log messages.

Snort architecture is broken into four parts, i.e., Packet Sniffer, Preprocessor, detection Engine, Alert/log and log files/Database [14]. Packet Sniffer sniffs the packet, and matches them again certain Preprocessor. Preprocessor checks for a certain plug-ins and search for a certain type of behavior and send it to detection engine. The action is basically performed in a detection engine mode where the rule is applied on each packet and search for a certain type of behavior of known attacks. The Snort rule-set could be downloaded directly. Rules are broken into two logical areas: rule headers and rule options. Rule headers contain required protocol fields that every rule must have and rule options contain a list of optional information used to refine a match and the rule action tells Snort what to do when a match occurs. The rule field format and an example rule are as follows:

<action><protocol><sourceIP><sourcePort><direction> <destIP> <destPort> (<rule options>)

If the packet matched against a rule several actions could be performed, i.e., alert, log, pass, activate. In this project we use alert and log action to detect an attack and log it. Alerts are stored in database MySQL or it could be displayed exhibit using SNORBY (an open source GUI interface for SNORT).

3.3 Machine Learning

Machine learning evolved from artificial intelligence (AI), provides a program with the capability to learn without being explicitly programmed, it also focuses on the development of computer programs that can teach and learn themselves to grow and change when exposed to new data [23]. In this project, the ML based approach is used to eliminate false positives and false negatives from the system. A false positive is a type of an alert that triggers on average traffic where no intrusion or attack is underway which is an issue in rule based NIDS, a false negative, defined as the failure of a rule to trigger when an actual attack is an underway which also occurs in the rule-based NIDS [21].

3.3.1 Sequential Minimal Optimization (SMO)

Sequential minimal optimization (SMO) is a machine learning algorithm for solving the quadratic programming (QP) problem and optimization problem that occurs during the training of support vector machines [6]. SMO is widely used for training, support vector machines and is applied by the LIBSVM tool. SMO breaks the problem into a chain of smallest possible sub-problems, which are then solved analytically.

3.3.2 J48 Decision Tree Classifier

J48 Decision Tree algorithm is an extension of ID3 algorithm, and is used to find out the patterns the attributes behaves for a number of instances. This algorithm generates the rules for the prediction of the target variable.

The additional features of J48 are accounting for missing values and decision trees pruning. In the WEKA data mining tool, J48 is an open source Java implementation of the C4.5 algorithm [26].

3.3.3 Simple Logistics

Simple logistic is a statistical method for analyzing a dataset in which there are one or more independen variables that determine an outcome. The outcome is measured with a dichotomous variable (in which there are only two possible outcomes) [26].

3.4 KDD Dataset

Intelligent Intrusion detection systems can only build if there is an availability of a valid data set. A data set with the sizable amount of data which mimics the real-time can only help to train and test an intrusion detection system. In our case, we used The KDD data set to build our intrusion detection system model. There are 42 attributes in KDD dataset [12].

4. Approach / Experimental Setup

The methodology of the project is to set up a hybrid network intrusion detection system by using two different approaches i.e., rule/signature-based and anomaly/machine-learning based NIDS with real-time data as input. To construct a hybrid NIDS, we implemented a rule-based NIDS and Machine Learning classifiers in series. SNORT collects real-time network data and classify them as an intrusion or normal packet, and stores this information into MySQL database. Finally, trained machine learning models are used to further validate the prediction results of SNORT. The validation process reduces the false positives/negative rates of rule-based NIDS. The overall architecture of our proposed hybrid network intrusion system is shown in Figure 1.

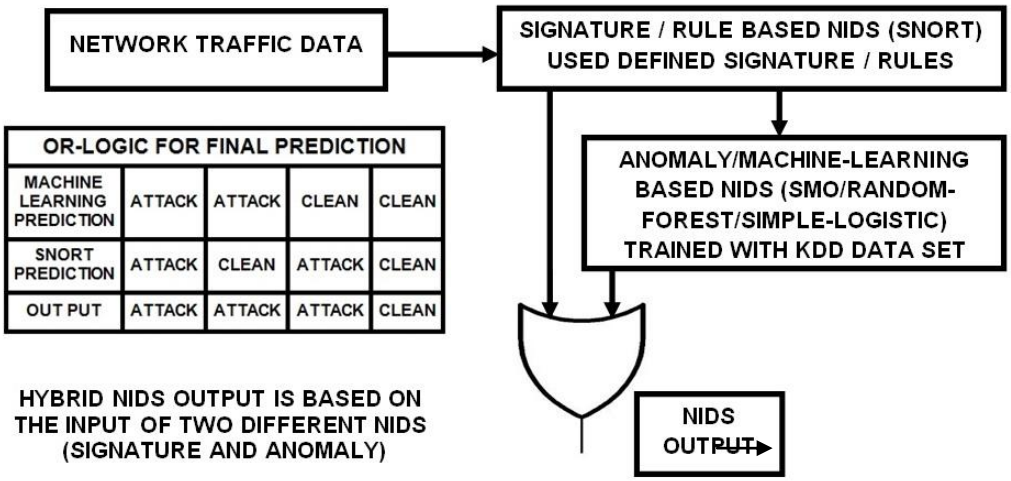

Figure 1. Architecture of the Proposed Hybrid NIDS

4.1 Rule-Based Network Intrusion Detection System

We used SNORT as Rule-Based NIDS to collect real-time data. For this purpose, we configured SNORT on Linux system (ubuntu14.04 LTS). Although, SNORT provides built-in rule-sets for the detection of known attacks, but we upgraded its detection system which allowed us to write our own rules. To do so, we used different rules, like, we used rule to detect icmp-event, and also wrote a simple PING rule to test SNORT. We used a command prompt to verify and collect SNORT ping's data (clean). Then we defined another rule for the collection of malicious or intrusion data by generating DOS attack.

a) *alert tcp any any -> any any (msg:"ICMP test detected"; GID:1; sid:1000001; rev:001; classtype:icmp-event;)*
b) *alert tcp !$HOME_NET any -> $HOME_NET any (flags: S; msg:"Possible TCP DoS"; flow: stateless; threshold: type both, track by_src, count 70, seconds 10; sid:10003;rev:1; classtype:denial-of-service;)*

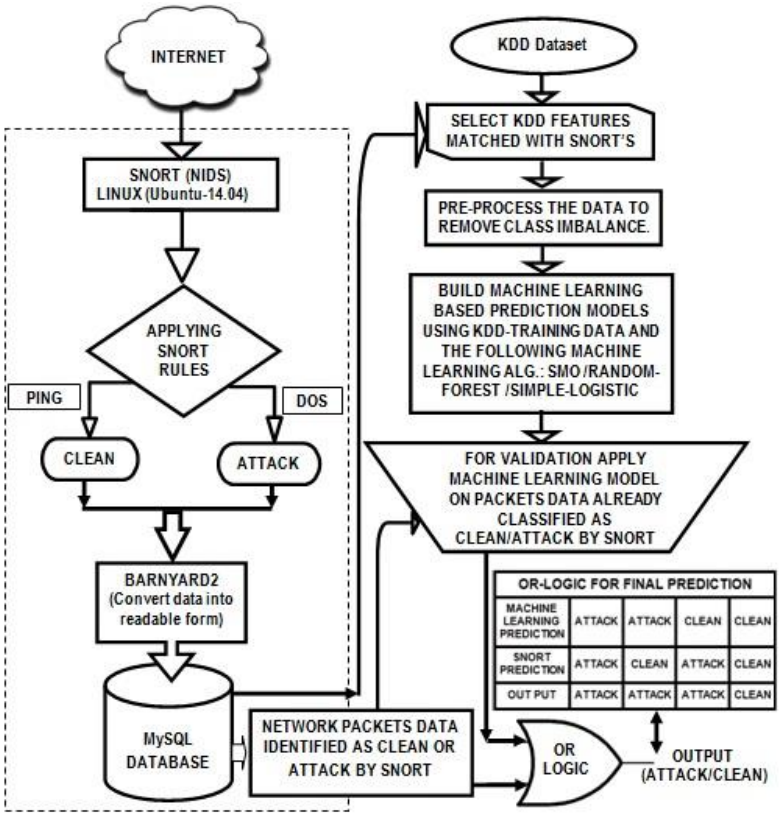

Figure 2. Hybrid NIDS Using Machine Learning Classification And Rule-Based System

Since, SNORT collects data in binary form, therefore, to convert the data in a human readable form, Barnyard2 (tool) was used which stored data in MySQL database [15][16], we converted the stored data into CSV format. Afterward, the CSV files containing SNORT data imported into a new database, because SNORT has its own schema for storing data, we wrote a query to relate the data and form a SNORT VIEW which labeled packet's data as ATTACK and CLEAN. Finally, we used the SNORT VIEW data as input to 03 different trained machine learning classifiers (i.e., SMO, J48 and Simple Logistic) to further validate the output results of SNORT (a rule based NIDS). The output of the two NIDS is used as input to our hybrid NIDS which predict final output using OR logic on input data. The overall system process flow diagram is shown in Fig.2.

4.2 Machine-Learning-Based Network Intrusion Detection System

For Machine Learning based packets' classification, we first trained and tested the SMO (support vector machine), J48 classifier and Simple Logistic models using freely available KDD dataset. KDD data set 42 features, but we selected only those features which were similar with the extracted features sets of SNORT. These selected features were used to train all the models. The list of selected common features in both KDD and SNORT are shown in Table-1.

Table 1. Common Features In Kdd And Snort Database

Sr. No.	Features Names
1	PROTOCOL
2	FLAG
3	COUNT
4	DURATION
5	CLASS

Before training and testing of SMO, J48 and Simple Logistic models, different class imbalance techniques were also considered to improve the model performance because NIDS data is mostly class imbalance [25]. The classification results of the three models are shown in Table 2. In case of J48 (Tree Classifier), and SMO the precision, recall, and F-measure values of "Anomaly" class are more than 92%.

Table 2. Classification Performance Of SMO, J48 and Simple Logistic Models Trained With Kdd Dataset

MACHINE LEARNING CLASSIFIERS	CLASS TYPE	PRECISION (%)	RECALL (%)	F-MEASURE (%)
SMO	Normal	93.1	93.2	93.1
	Anomaly	92.2	92.1	92.2
J48	Normal	94.2	97.8	96.0
	Anomaly	97.4	93.1	95.2
Simple Logistic	Normal	84.6	95.0	89.5
	Anomaly	93.4	80.3	86.4

5. Results And Discussion

To obtain the final classification results of our proposed hybrid model, we used the trained model of machine learning to validate the network packet data which were already classified by SNORT. The prediction model of SMO is shown below, which was used in our experiment to validate the classification results of SNORT. The overall prediction of the hybrid system is shown in Table 3 which is based on OR gate logic.

Prediction model = 0.0018 × (normalized) duration + (-0.6667) × (normalized) protocol_type=tcp + -0.6671 × (normalized) protocol_type=udp + 1.3338 × (normalized) protocol_type=icmp + (-1.2726) × (normalized) flag=SF + 0.728 × (normalized) flag=S0 + 0.7279 × (normalized) flag=REJ + 0.7262 × (normalized) flag=RSTR + 0.7278 × (normalized) flag=SH + 0.7279 × (normalized) flag=RSTO + -1.2738 × (normalized) flag=S1 + 0.727 × (normalized) flag=RSTOS0 + -1.273 × (normalized) flag=S3 + -1.2727 × (normalized) flag=S2 + 0.7273 × (normalized) flag=OTH + 0.001 × (normalized) count + 0.9395

Table 3. Output of The Hybrid NIDS System Using "OR-Gate" Logic

SNORT Prediction	SMO Prediction	Hybrid System Prediction
ATTACK	ATTACK	ATTACK (Reduced the probability of false positive rate)
ATTACK	CLEAN	ATTACK (with probability of false positive)
CLEAN	ATTACK	ATTACK (with probability of false negative)
CLEAN	CLEAN	CLEAN (Reduced the probability of false negative rate)

We used OR gate logic at the output of both the systems to identify an attack more accurately. If SNORT identifies a packet as an ATTACK and Machine Learning identifies it as CLEAN then we classify that packet as an ATTACK with high probability of false positive rate. However, if both systems classify a packet as CLEAN, only then it will be considered as CLEAN. In this way, our approach will be strong and can be flexible according to the network activity. A sample of classification results of the hybrid system is shown in Table 4, which depicts that with the help of OR gate logic we can improve the reliability of network intrusion detection system.

Table 4. Sample Data (Examples) of the Final Results Of the Hybrid NIDS System

S. No	PACKET DETAILS	SNORT RESULTS	ML RSULTS	FINAL RESULTS
1	Packet type:icmp,cid:2	icmp-event, clean	clean	Clean
2	Packet type:ip,cid: 8514	bad- unknown, attack	clean	Attack
3	Packet type:ip,cid: 3	icmp-event, clean	attack	Attack
4	Packet type:ip,cid: 10406	Sdf, attack	attack	Attack

6. Conclusion

The implemented hybrid NIDS system is based on two different learning approaches, i.e., rule-based learning system and machine learning classifications. We used SNORT as rule-based system and SMO, J48 and Simple Logistic as machine learning classifiers. The advantage of using multiple intrusion detectors is that no intrusion or malicious behavior is missed i.e., defense-in-depth. Our proposed system detects security threats and attacks by providing real-time network monitoring. The results of both the learning approaches were compared using OR-gate logic, which resulted in successfully reducing the number of false positive and false negative rates. In future we will work to further enhance our approach and build open source software based on our hybrid network intrusion detection system.

References

[1] D. E. Denning, "An Intrusion-Detection Model", IEEE Transaction on Software Engineering, vol. 13, no. 2, **(1987)**, pp. 222-232.
[2] T. F. Lunt, "Detecting Intruders in Computer Systems", Sixth Annual Symposium and Technical Display on Physical and Electronic Security, Philadelphia, **(1993)**.
[3] H. S. Vaccaro and G. E. Liepins, "Detection of Anomalous Computer Session Activity", The IEEE Symposium on Security and Privacy, **(1989)**.
[4] C. Dowell and P. Ramstedt, "The Computer Watch Data Reduction Tool", Proceedings of the 13th National Computer Security Conference, **(1990)**; Washington, D.C..
[5] F. Gilham Jr., Dr. Neumann, A. Valdes, T. F. Lunt, A. Tamaru, R. Jagannathan, C. Jalali, H. S. Javitz and T. D. Garvey, "A Real-Time Intrusion-Detection Expert System (IDES)", SRI International Project, **(1992)**.
[6] S. Mukkamala, G. Janoski and A. Sung, "Intrusion Detection: Support Vector Machines and Neural Networks", Proceeding of IEEE International Joint Conference on Neural Networks, **(2002)**.
[7] J. E. Díaz-Verdejo, G. Maciá-Fernández and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges", computers & security, vol. 28, no. 1, **(2009)**, pp. 18-28.
[8] V. Das, V. Pathak, S. Sharma, M. Srikanth and G. Kumar, " Network intrusion detection system based on machine learning algorithms", **(2010)**.
[9] A. S. Geetha, T. S. Indhur and S. Bose, "Hybrid network intrusion detection system using expert rule based approach", Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, **(2012)**.
[10] K. Satpute, S. Agrawal, J. Agrawal and S. Sharma, "A survey on anomaly detection in a network intrusion detection system using particle swarm optimization based machine learning techniques", Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), **(2013)**.
[11] Z. Malek and B. Trivedi, "The Rule Based Intrusion Detection Model For User Behavior", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 12, **(2015)**.
[12] L. Dhanabal and D. S. P. Shantharajah "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms", International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, no. 6, **(2015)**.
[13] Roesh, "Lightweight Intrusion Detection System", Proceedings of LISA: 13th Systems Administration Conference, **(1999)**.
[14] B. Caswell, J. Beale and A. Baker, "Snort IPS and IDS Toolkit", Syngres publisher, **(2007)**, pp. 76-81.
[15] R. U. Rehman, "Intrusion detection systems with Snort: advanced IDS techniques using Snort, Apache, MySQL, PHP, and ACID", pp. 157-176.
[16] N. Dietrich, "Snort 2.9.8.x on Ubuntu 12, 14, and 15 with Barnyard2, PulledPork, and Snorby", **(2015)**.
[17] K. Hwang, M. Cai, Y. Chen and M. Qin, "Hybrid intrusion detection with weighted signature generation over anomalous internet episodes", IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 1, **(2007)**, pp. 41–55.
[18] J. Gomez, C. Gil, N. Padilla, R. Banos and C. Jimenez, "Design of a snort-based hybrid intrusion detection system," Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing, and Ambient Assisted Living, pages 515–522, Springer, Berlin, **(2009)**.
[19] J. Beale, A. R. Baker and J. Esler, "Snort: Intrusion detection and Prevention Toolkit", Syngress, **(2007)**.
[20] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning For Network Intrusion Detection", IEEE symposium on security and privacy, **(2010)**.
[21] S. N. Shah and M. P. Singh, "Signature-Based Network Intrusion Detection System Using SNORT And WINPCAP", International Journal of Engineering Research and Technology, ESRA Publication, **(2012)**.
[22] Ö. Cepheli, S. Büyükçorak and G. K. Kurt, "Hybrid Intrusion Detection System for DDoS Attacks", Journal of Electrical and Computer Engineering, vol. 2016, **(2016)**.
[23] K. Sravani and P. Srinivasu, "Comparative Study of Machine Learning Algorithm For Intrusion Detection System", Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), **(2014)**.
[24] F. Cohen, "Computer Viruses", International Journal on Computers Security, vol. 6, no. 1, **(1987)**, pp. 22-35.
[25] F. Rahat and S. N. Ahsan, "Comparative study of machine learning techniques for pre-processing of network intrusion data", International Conference on Open Source Systems & Technologies (ICOSST), **(2015)**; Lahore.
[26] I. H. Witten and E. Frank, "Data Mining: Practical Machine Learning Tools and Techniques, Third Edition", **(2011)**.

Authors

Ezzat Batool is a Final year student of B.E (Telecommunication Engineering) at the Faculty of Engineering Science and Technology (FEST), Iqra University (IU), Defence View (Main Campus), Shaheed-e-Millat Road (Ext.) Karachi-75500, Pakistan. Her research interests includes machine learning application in Telecom industry and network security. She has recently completed her B.E final year project on hybrid network intrusion detection system.

Urooj Aslam is a Final year student of B.E (Telecommunication Engineering) at the Faculty of Engineering Science and Technology (FEST), Iqra University (IU), Defence View (Main Campus), Shaheed-e-Millat Road (Ext.) Karachi-75500, Pakistan. Her research interests are in cyber security and ruled based network intrusion detection system. Like SNORT. She has recently completed her B.E final year project on hybrid network intrusion detection system.

Abdullah Sultan is a Final year student of B.E (Telecommunication Engineering) at the Faculty of Engineering Science and Technology (FEST), Iqra University (IU), Defence View (Main Campus), Shaheed-e-Millat Road (Ext.) Karachi-75500, Pakistan. His research interest is in network intrusion detection system. He has recently completed his B.E final year project on hybrid network intrusion detection system.

S. N. Ahsan is working as Associate Prof. at FEST, IU, Main Campus since 2011. He did his PHD in Machine Learning application in Software Engineering from GRAZ University of Technology, Austria in 2010. His Research interests includes software maintenance, software evolution, cyber security, network intrusion detection system and machine learning. Currently he is supervising MS/PHD students in Computer Science and Telecommunication Engineering at FEST, IU campus Karachi.