INTERNATIONAL JOURNAL OF SCIENCE

ISSN: 2455-0108 | WWW.IJOSCIENCE.COM

VOLUME II ISSUE II APRIL 2016

A Hybrid Approach of Intrusion Detection System Based on Neural Network and Normalization

Kavita Patil, Dr. Bhupesh Gour, Mr. Deepak Tomar

Department of Computer Science & Engineering

Technocrats Institute of Technology, Bhopal
RGPV University Bhopal, INDIA

Abstract— In the whole world, the most famous threat that are spread around is done by the intruder computers over the internet. The types of external activity found over the system are termed as intrusion and the mechanism that is applied for the preservation of the information against these intrusions are called as intrusion detection system. For protecting the network, first there is a need to detect the attacks then take the proper action regarding it. There are techniques applied for scanning and analysing for highlighting the susceptibilities and loop-holes within the components of security, various aspects of network that are not secured and also implementation of the intrusion-detection and prevention-system techniques are also described here. In this paper, proposed methods based on Neural Network is described that provides better way of attack detection, that are required in various applications of security such as network forensics, portable computer and the event handling systems by applying various different approaches. Proposed work is implemented in MATALB.

Keywords- Intrusion, Detection, Attacks, Neural Network, KYOTO.

I. INTRODUCTION

In current world the most of the contents of users are based on internet so the users are also considered as the content by the system [1], [2]. By the growth of the internet and the sharing of the information and contents over the internet by the users there are numerous growth have been observed in the expansion of the computer network and its effect over the social web. With the raise in the number of users sharing the contents over the internet and get accessed over it may now become the base for the advancement of the global culture which is influencing the life of the people personally and commercially both. So there is a need to protect these shared contents of the internet against the intruders that enters into the systems to obtain the personal data, steal their passwords, or all types of misuses which they may perform over the system.

There are mainly three types of the aspect that are considered for the security of the system, these aspects are: confidentiality, integrity and availability respectively. In which the confidentiality confirms the protection of the information.

With the increase in the development of the communication networks along with introducing various technologies, also there have been raised several unwanted possibilities of attacks over the network. In the radio access networks, the threats more found as these networks are more susceptible. With the increase in the complexity level of the threats this implies the requirement of the more advance and intelligent system for the security system. Though, the traditional methods of security are not having the capacity to cope up with the current more advanced form of threats that are rising over the internet. By increasing the layers of security in the intrusion-detection-system the more enhanced solution to the security of networks get created [3.]

All the events get monitored by the intrusion-detection-system that are found in the computer system or the network then get analysed for the detection of the signs of the intrusions by the system of intrusion detection. One of the security management systems are the intrusion detection for the computer and the networks. This intrusion-detection-system analyse the information that are collected from the various sources of the network to recognize the security breaches that are possible in both forms as an intrusion which is the type of attack that are performed from outside of the organization and the misuse that is the attack carried out from the inside of the system. The network based intrusion-detection-system includes the set of sensors or the host systems that are situated at many locations within the network. In this system the traffic of the network gets monitored, then analyse these traffics and inform about these attacks to the management. There are normally two types of network-based-intrusion detection, first is rule-based and second is anomaly-based intrusion detection [4].

The major issue of the intrusion-detection-system is the high rate of false-positive alerts. Perfect intrusion-detection-system never creates the false or irrelevant alarms. Whereas the signature based intrusion detection may generate more rate of false alarms due to lack of verification tool and the common signature used.

II. INTRUSION DETECTION SYSTEM

The system that is behave as the methods, mechanisms, tools to recognize the resources and reporting the misbehaviour or unusual activity over the network are known as the intrusion-detection system. Among the whole mechanism of the IDS system the intrusion detection is the one part which provides the detection of the intrusions in the network in order to provide the protection to the designed system. This system also has a history behind the reason of introducing this system. There are two types of approaches have been observed in this system such as anomaly based intrusion-detection-system and the misuse based intrusion detection system [5].

Basic concept of the misuse detection represented in the manner such that the attacks having various form or pattern or signature got detected even they are having the variations of these attacks may also got detected. Depending on the given signatures, this technique recognized the attacks among the huge rules sets that are providing the information about each type of known attack. Main demerit of this method is complexity for recognizing the unknown attacks that are found over the network. Main objective of the anomaly-detection is to design statistical model that describes the normal-traffic.

In the approach called pattern matching encodes the signatures of known intrusion as the patterns which are get matched with the audit data after detection. And the intrusions signatures are also categorized by using the inter-relationships in between the components of signatures. And these types of structural inter-relationships are then measured over the high-level of events that are also defined as the low-level audit-trail incidents or events.

And this type of classification of the signatures of intrusion is not dependent on any given framework of the pattern matching for computation. In this patterned signatures got matched with audit-trails records if any of the matched patterns got detected as the intrusion then the intrusions may be characterized according to the structure of the events that are required to find them.

Based on techniques that are used for the detection, the intrusion detection systems may be categorized as [6]:

- Signature or misuse-based intrusion detection systems
- Anomaly-based intrusion detection systems
- Specification or hybrid-based intrusion detection systems

In case the company is planning to implement any of the intrusion-detection-system then it must determine the available resources for operation of the systems and also for their maintenance that are required [7]. The complete lifecycle of the mechanism for the efficient intrusion-detection-system is performed. Here the complete process explained the observations of intruder along with the work that is needed for the maintenance of system within network along with the traffic also the process of selection explains regarding the recognition of the approaches, character, accuracy, effectiveness and usability of the system.

III. INTRUSION DETECTION V/S PREVENTION SYSTEM

The process of intrusion-detection is described as monitoring of the activities that are found within the system or a computer or various networks. And the procedure which is carried out this complete work is referred as Intrusion-Detection-System [8]. The intrusion-detection-system is also termed as the burglar-alarm. Like an example in the home most commonly used lock system in order to protect the home from being got theft. Still if a person breaks lock system in order to attempt to get enter into the house, then the burglar-alarm detects the lock which has been got broken and then it informs the owner of the house through generating an alarm which may be in any form like email, message in mobiles etc.

The intrusion-prevention-system is also a security/threat prevention technique for the network which monitors the traffic flows of the network to identify and secure the network’s susceptibility that is presented. Very easy rule for security of the network is the defence-in-depth that is that layered based solution provides the security to the information over the network against the malignant attacks by applying the intrusion-detection and prevention system. And after selecting the proper intrusion-detection and prevention mechanism, it then gets deployed efficiently to the entire company [9].

This type of task is carried out by the design and architecture of the intrusion-detection and prevention policies and through declaring their policy. The signature based mechanism is the one that works for identifying the particular patterns of thee event or the behaviour which proceeds along with the threats. And the host-based IDPS is generally got applied within the software that are situated on the top of operating-system.

On the contrary, this system is dependent on events that are gathered through the hosts which they are monitoring. And its main functionality is the monitor the internal functioning of host like sequence of the system calls that are made, and the file that got accessed also the other approaches that are using these systems or the application-logs with the working of the operating system information to recognize the efficient events for an intrusion. Whereas, the network-based intrusion detection-prevention-systems collects the input data through monitoring the traffic of network such as the packets that are collected through the network interfaces within the promiscuous state [10].

The intrusion-detection-system is normally stores the information that are associated to the recorded events, to inform the security administrators regarding the significant events that are observed and generated the reports. Various intrusion-detection-systems also provide the response to the identified threat through preventing it from affecting the system.

IV. LITERATURE REVIEW

In this paper [11] based on the analysis proved the Probabilistic-Neural-Networks to be as the approach which is providing better accuracy than the other type of Neural-Networks such as the Feed-Forward Neural-Network, Generalized-Regression Neural-Network, Elman-Neural-Network and the Radial-Basis Neural-Network. In this paper suggested the decrease in the feature matrix provides the improved performance. Hence the accuracy increases the efficient feature-selection approaches which may be implemented for enhancing the accuracy of the system. Here the clustering approaches have been used for recognizing the less frequent-data for better consideration. Therefore, it is proved the more rate of accuracy for the suggested approaches.

In this paper [12] depending on the genetic algorithm suggested a fuzzy logic along with the data-mining approach that is one of the approach of class-association rule-mining. Because of the fuzzy-logic the suggested approach may work with the mixed attributes which also ignore the issue of sharp boundary. In this system the genetic-algorithm is implemented to generate various rules that are needed for the anomaly based detection systems. Also here association-rule-mining is implemented to derive the enough significant rules for the use of the users to derive the rules that are fulfilling the all the conditions that are essential for the misuse-detection approach for detecting the intrusive behaviour of the system also decreases the rate of false-alarm through this approach.

In this paper [13], suggested the mechanism for providing one of the best approaches for the intrusion detection in order to provide the security of the network. Hence, this is obtained through decreasing the false-alarm-rate and enhancing the detection rate of the system through applying the fuzzy rule base. This suggested system may also monitor the asperity of the attacks. And through understanding the levels of the attack the decisions can be build on them. Also based on the levels of the attacks the action will be performed by the use of intrusion-preventive-system.

This paper [14], point out the significance of designing
the efficient intrusion-detection-systems to defeat the attacks
against the cognitive-radio-networks. In this also, suggested an effective intrusion-detection-system that may be applied within the cognitive radio software of the secondary users. This suggested approach of intrusion-detection-system may apply the non-parametric cu sum-algorithm also that provides the anomaly based detection system. In this paper through understanding the usual mode of the functioning the parameters of the system of the CRN, suggested system is now capable to identifying the malicious behaviour which causing from the attack.

[15] Within this suggested an effective approach to resolve the issue of the intrusion that are found in network and which has been also complicated to detect. So in this paper the Denial-of-Service attack which affects the large volume of the computers daily got analysed and detection mechanism have been suggested for this and also the forestalling of computers have been obtained. In this paper for achieving this objective a genetic-algorithm based method have been used for the preparation of the policy to detect the DoS attacks over the network. For this GA is applying on the KDD trophy 99 dataset’s facts set to create an imperative-set which are maintained to detect the attacks on the network.

[16] Here various effective algorithms have been reviewed for the intrusion detection approach which is dependent on the several techniques of machine learning. For designing a best intrusion-detection-system all the features of the machine learning support it which have the high rates of detection and the less

rates of false positive whereas this system get accepted quickly for any change in the malicious activities. In regards of this the machine learning approach is divided into two types first one is Artificial-Intelligence (AI) and second is Computational-Intelligence (CI). In which the various properties of the CI-based approach, like fault tolerance, adaptation, high computational speed or the error resilience regarding the noisy information, ensures the need for creating an effective system for intrusion detection.

In this paper [17], approach for the intrusion-detection has been represented through using the k-means clustering, C 4.5 and fuzzy neural network. Also with the support of the k-means clustering approach, to build the huge training data-set which is heterogeneous in nature which is then sub divided into the more subsets. In the form of result this subdivision the complexity of every subset gets decreased and simultaneously increases the performance of detection. Following the starting stage of clustering the training dataset may be then provided to the fuzzy-neural network which then provided to the classification by the use of C 4.5 decision tree. In this the result obtained by C 4.5 is much better than the Support Vector Machine approach.

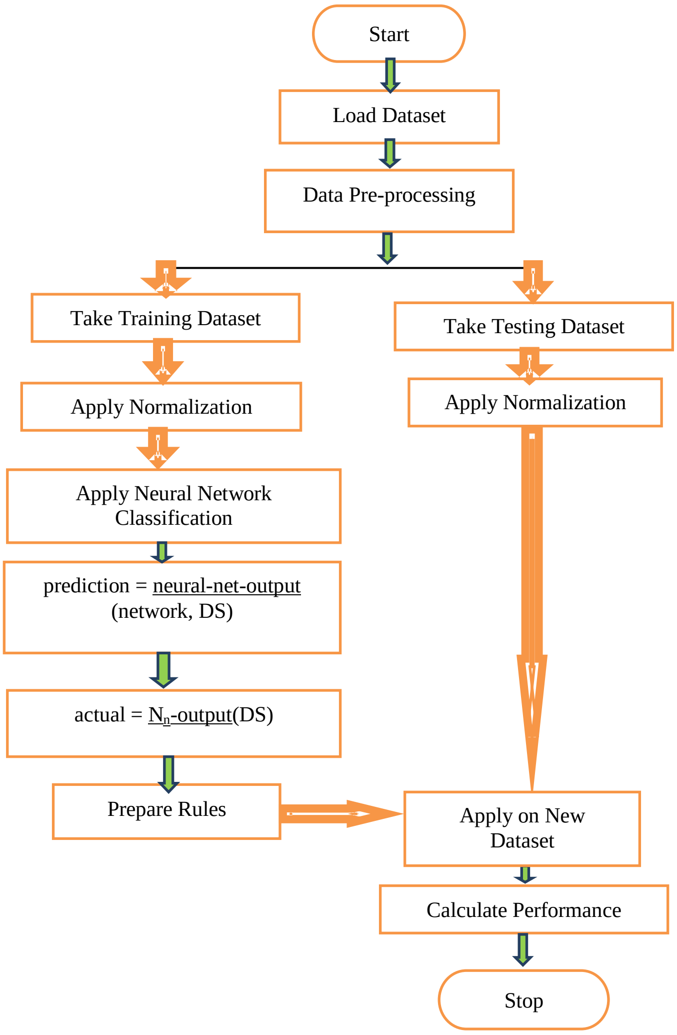
In this paper [18], suggested the widely used data mining approach for the network-intrusion-detection system through deriving the useful knowledge among the huge data obtained from network. Here the hybrid model is also suggested which merges the anomaly-based-intrusion detection along with the signature-based Intrusion-detection which is then break down into two separate phases. Initial phase includes the signature based intrusion detection in which the SNORT algorithm is applied to produce the alerts for the anomaly data. And the second phase includes the data mining approach in which the “k-means + CART” is applied to cascade the k-means clustering approach along with the Classification-and Regression-Trees approach in order to classify the normal activities and the abnormal activities separately. Here the KDD Cup dataset is applied for the analysing the hybrid intrusion detection in order to provide low rate of false positive.

V. NEURAL NETWORK IN CLASSIFICATION

The most interesting domain of research for the neural network is the Classification. These neural networks are the form of electronic networks that are made up of neurons which is much similar like the neurons of brain. In this system single record gets processed at one time, and it is get known through comparing the record of classification of huge amount with the existing record of classification. In this process the generated error in the starting phase of the classification get back to the network for modification of the network in further iterations. The artificial neural networks are designed on the basis of the basic concept of the neural network of the human brain, which is made up of small units called as neurons with the connection between these neurons. This connection between the neurons is used to evaluate the performance of the behavior of network. For selecting the type of network is decided on the basis of the issue which needs to be solved and the back-propagation gradient network which is used commonly.

VI. MULTILAYER PERCEPTRON CLASSIFICATION OF NETWORK INTRUSION DETECTION SYSTEM

This section talks about the proposed work. This proposed work is concentrate on Multilayer Perceptron based Neural Network for Intrusion Detection. Figure 1 shows the flow chart of the proposed work as shown below:



Proposed work’s algorithm is shown below:

A. File read

```
1. Load DS
2. Read and save DS n*m-1.
3. Read and save Class m for performance calculation
```

B. Preprocessing

```
1. Convert string m to integer m
      if DS (n, m) == stringt
         stringt == integert
      if end
2. Normalize DS n*m except Class m
      DSnm = $\frac{Xi-Min(X)}{Max(X) - Min(X)}$
3. Make target inputs with Class m
      if Nn == Class m
            Nn (n, N) = 1
      else
            Nn (n, N) = 0
      if end
```

C. Multilayer Perceptron (Neural Networks)

```
1. For training DS
2. prediction = neural-net-output (network, DS)
3. actual = Nn-output(DS)
4. compute error (prediction - actual) at the output units
5. compute   for all weights from hidden layer to output layer
6. compute   for all weights from input layer to hidden
7. update network weights //input layer not modified by error estimate until all examples classified correctly or another stopping criterion satisfied
8. return the network
9. Calculate Performance
```

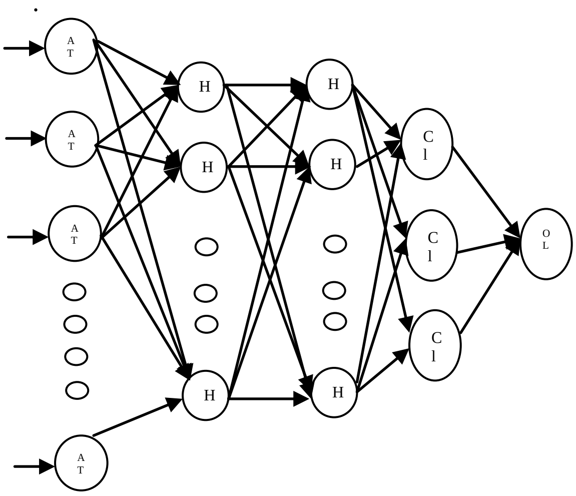


Figure 2: Working of Neural Network

WORKING OF NEURAL NETWORK

In neural network, first layer is input layer which is having attribute value in input. There is connection of some weights with first hidden layer. This is assigned to train first hidden layer in connection with third layer and so on. This happens till last hidden layer. It is having only three perceptron corresponding to number of class. Last hidden layer is connected with output layer. This neural network learns its weight in training time. While testing they are used. The working of the Neural Network is shown in figure 2.

VI. RESULT ANALYSIS

This section talks about the result analysis along with the system configuration and the dataset on which experiments are performed.

Dataset

This work has used Kyoto 2006+ Network Intrusion Data Set. There are total 40000 no. of rows used. Total no. of columns used is 14 along with the class discrimination attribute. There are total three type of records in dataset.

The detail of the dataset is as follows:

Table I: Detail of KYOTO dataset

S. No.	Feature	Description
1	Duration	Length of the connection
2	Service	connection’s service type, e.g., http, telnet, etc
3	Source bytes	number of data bytes sent by the source IP address
4	Destination bytes	Number of data bytes sent by the destination IP
5	Count	the number of connections whose source IP address and destination IP address are the same
6	Same srv rate	% of connections to the same service in Count feature
7	Serror rate	% of connections that have “SYN” errors in Count feature
8	Srv serror rate	% of connections that have “SYN” errors in Srv count feature
9	Dst host count	among the past 100 connections whose destination IP address is the same to that of the current connection
10	Dst host srv count	among the past 100 connections whose destination IP address is the same to that of the current connection
11	Dst host same src port rate	% of connections whose source port is the same to that of the current connection in Dst host count feature
12	Dst host serror rate	% of connections that have “SYN” errors in Dst host count feature
13	Dst host srv serror rate	% of connections that “SYN” errors in Dst host srv count feature
14	Flag	the state of the connection at the time the summary was written

System Configuration

The system on which experiments are performed is as follows:

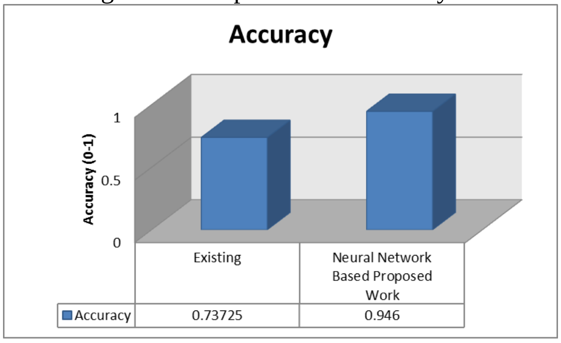
Model:	Sony Vaio
Processor:	Intel® Core™ I5-2450M 2.5GHz
RAM:	4GB
System Type:	64 Bit Operating System
Windows Edition:	Windows 10 Home
MATLAB	R2014a

Result Analysis

While executing various experiments, data is divided into two parts one is called training data and another is called testing data. The ratio which is maintain for this experiments is 50-50%. It means 50% data is divided for training purpose and rest 50% is used for testing purpose.

Table I: Accuracy Results

Figure 1: Comparison of Accuracy Results



Here Table I along with figure 1 shows the comparative study of the accuracy results.

Table II: F measure Results Comparison

	Existing	Neural Network Based Proposed Work
F measure	0.323047	0.865287

Table II along with the figure 2 show the comparative results of the f-measure of the existing work in comparison of proposed work.

	Existing	Neural Network Based Proposed Work
Accuracy	0.73725	0.946

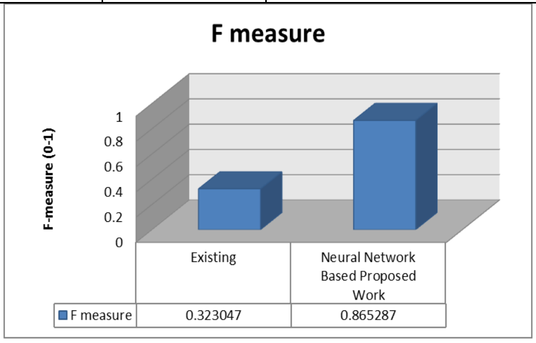


Figure 2: Comparison of F Measure Results

VII. CONCLUSION

This method paper is concluded by describing the various intrusion-detection-systems that are generally detects the attack signatures and then generates an alert. Here described several detection methodology and the approaches for the intrusion-detection-systems that are classified the intrusion-detection-system as the misuse-detection and the anomaly-detection systems. In this paper various different methods have been explained that are existing for the intrusion-detection-systems that may efficiently detect the malignant activities and which provide support in providing the protection efficiently. This proposed method is implemented in MATLAB. The results from table I & II clearly show the efficiency of the proposed work over the existing work.

REFERENCES

[1] Manish Somani1, Roshni Dubey2 "Hybrid Intrusion Detection Model Based on Clustering and Association" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 3, March 2014

[2] Ammar Boulaiche, "A Quantitative Approach for Intrusions Detection and Prevention Based On Statistical N-Gram Models ", Procedia Computer Science 10 (2012) 450 – 457.

[3] X. Zhang, L. Jia, H. Shi, Z. Tang and X. Wang,

"The Application of Machine Learning Methods to Intrusion Detection", Engineering and Technology (S-CET), 2012 Spring Congress on, (2012), pp. 1-4.

[4] Y. Jiao, "Based on Data Mining in Intrusion Detection System Study", International Journal of Advanced Computer Science, vol. 2, (2012).

[5] Yuh-Jye Lee," Anomaly Detection via Online Oversampling Principal Component Analysis", IEEE VOL. 25, NO. 7, JULY 2013.

[6] Hesham Altwaijry, "Bayesian Based Intrusion Detection System ", Journal of King Saud University – Computer and Information Sciences (2012) 24,1–6.

[7] John McHugh, Alan Christie, and Julia Allen- "The Role of Intrusion Detection Systems"- Software Engineering Institute, CERT Coordination Center

[8] Deepak Upadhyaya and Shubha Jain, "Hybrid Approach for Network Intrusion Detection System Using K-Medoid Clustering and Naïve Bayes Classification", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, pp 231-236, May 2013

[9] Mugdha Kirkire, Poonam Gupta" Intrusion Detection in Mobile Ad-hoc Network" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, pp. 869-876, February- 2014.

[10] Modi C, et al. 2012, ―A survey of intrusion detection techniques in Cloud‖, Journal of Network and Computer Applications,

[11] Wasima Matin Tammi, Noor Ahmed Biswas, Ziad Nasim, Khadizatul Zannat Shorna, Faisal Muhammad Shah, "Artificial Neural Network based System for Intrusion Detection using Clustering on Different Feature Selection", International Journal of Computer Applications (0975 – 8887) Volume 126 – No.12, September 2015.

[12] R. Ravinder Reddy, Dr. Y Ramadevi, Dr. K. V. N Sunitha, "Fuzzy Logic and Genetic Based Intrusion Detection System", Volume 5, Issue 8, August 2015 ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering.

[13] Bindiya Bansal, Kulwinder Singh, "Rule Based Intrusion Detection System to Identify Attacking Behaviour and Severity of Attacks", Volume 5, Issue 1, January 2015 ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering.

[14] Zubair Md. Fadlullah, Hiroki Nishiyama, Nei Kato, and Mostafa M. Fouda, "Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks," IEEE Network Magazine, vol. 27, no. 3, pp. 51-56, MayJune 2013.

[15] Sunil Kumar, Surjeet Dalal, "Optimizing Intrusion Detection System using Genetic Algorithm", International Journal of Research Aspects of Engineering and Management ISSN: 2348-6627, Vol. 1, Issue 1, FEB 2014, pp. 42-45.

[16] Mahdi Zamani and Mahnush Movahedi, "Machine Learning Techniques for Intrusion Detection", arXiv:1312.2177v2 [cs.CR] 9 May 2015.

[17] Meghana solanki, Vidya Dhamdhere, "A Hybrid Approach for Intrusion Detection Using Data Mining", International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 7, July 2015

[18] Jaina Patel, Mr. Krunal Panchal, "Effective Intrusion Detection System using Data Mining Technique", June 2015, Volume 2, Issue 6 JETIR (ISSN-2349-5162).