International Journal of Scientific Research & Engineering Trends
Volume 5, Issue5, Sep-Oct-2019, ISSN (Online): 2395-566X

Analysis of Embedded Network Security by Intrusion Detection System

Research Scholar
Mr. Suresh .B
Dept. of Electronics Erode Arts and Science College
Erode, Tamil Nadu, India
suresb@gmail.com

Associate Prof. & Head
Dr. M. Venkatachalam
Dept.of Electronics Erode Arts and Science College
Erode, Tamil Nadu,
India eacmvenkat@yahoo.com

Abstract **- Embedded devices are used to collect data; those devices include smart environments and autonomous systems. The increasing ability to connect, communicate with, and remotely control such devices via the legacy internet (IoT) has raised considerable security and privacy concerns. An Embedded network consists of several devices connected together to form a computing environment. In order to make security in embedded network, the connected device has to be secured. In this paper, the embedded device network security is analyzed with the help of Brain Storm Optimization (BSO) - Intrusion detection System (IDS) method to secure the embedded network from the attacks.**

Keywords **- Embedded Network, IoT, Intrusion Detection System, BSO, and Security.**

I. INTRODUCTION

Intrusion detection is defined as the process of observing the events occurring in a computer system or network and analyzing the violations or imminent threats of security policies or standard security practices violation. These violations may be caused by malware such as worms, spyware, virus, unauthorized access to the systems by some attacker, and authorized users misusing their privileges or flaws resulting in granting the attacker an elevated access to the network. An Intrusion Detection System (IDS) is software used for the automation of intrusion detection process. [1] IDS monitor network or system events for malicious activities that tend to compromise the confidentiality, integrity, and availability of network and send a report to the management station.

Intrusion detection refers to the process of monitoring the events happening in a computer system or network, examining them for signs of security problems. [2] The general meaning of intrusion detection reminds the analogous monitoring systems in other areas, including burglar alarms and video-monitoring systems found in banks and other renowned stores. Even the warning systems in civil defense and military fall into this functional category. Although the strategies employed are different in the various monitoring systems, yet the basic idea remains the same. The intrusion detection is defined as a process of detecting and responding to malicious activity directed at computing and networking resources. An IDS gathers and analyses the information within a network or a computer to perceive possible security fissures, which includes both attacks from Out side the organization and within the organization. It uses a technology, known as vulnerability assessment or scanning, for assessing the security of a computer or a network. The intrusion detection system procures data about information system to perform the analysis on the security status of that system. The foremost goal of IDS is to detect the security breaches, including both attempted breaches and potential breaches. A simple typical IDS is shown in the Figure.1

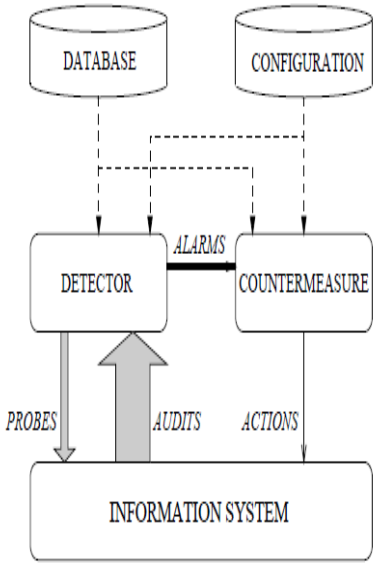

Fig.1. A Simple Intrusion Detection System.

An intrusion detection system is similar to a detector that processes information coming from the system to be protected. This IDS has the ability to launch probes that

can trigger the audit process, such as requesting version numbers for applications. It makes use of three categories of information: long-term information associated with the technique that is used to detect intrusions (such as a knowledge base of at tacks), configuration information that describes the present state of the system, and audit information unfolding the events that are happening on the system.

In order to ensure the proper functionality of the IDS, sensors are used to detect data, analyzers to evaluate data, panels to monitor activities, and user-interfaces to manipulate configuration settings. The IDS items can be in the form of packets, audit records of system, computed hash values or other data formats. Analyzers receive input from sensors and then determine the intrusive activity.

The efficiency of an intrusion detection system depends on the following parameters:

1. **Accuracy:** It deals with the proper discovery of attacks and the non-occurrence of false alarms.
2. **Performance:** It is the rate at which audit events are processed.
3. **Completeness:** It is the property of an intrusion detection system to identify all attacks.
4. **Fault Tolerance:** An intrusion detection system needs to be resilient to attacks, especially denial-of-service attacks.
5. **Timeliness:** An intrusion detection system has to accomplish and succeed its analysis as quickly as possible in order to empower the security administrator to respond before much damage has been done, and also to inhibit the attacker from subverting the audit source or the IDS itself [4].

Methods by which IDS automate the intrusion detection can be classified are false positives and false negatives. False positives are those sequences of innocuous events that IDS speciously classifies as intrusive, while false negatives refer to intrusion attempts that IDS fails to report. Detection of hostile attacks depends on both the number and type of suitable actions. Figure.2 describes the series of activities performed by an intrusion detection system.

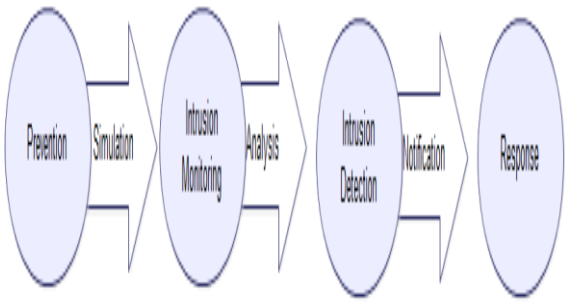

Fig.2. Activities of IDS.

IDS can be categorized into various types, on the basis of different monitoring and analysis approaches. IDS can monitor events at three levels:

Network-Network-based IDS (NIDS), presently the most common commercial product offering, detect attacks by capturing and analyzing the packets that navigate in a given network link. NIDS consists of a set of single purpose hosts that sniff the network traffic and report the attacks to a single management console. NIDS is secured against attack as no other applications run on hosts are used by it. These NIDSs have "stealth" modes which make it almost impossible for an attacker to detect their presence.

NIDS monitors the characteristics of network data and performs the intrusion detection. Most NIDS operate by examining the IP and transport layer headers of discrete packets, the contents of packets, or some other combination.

1. **Host-** Host-based Intrusion Detection System (HIDS) refers to the class of IDS that resides on a host machine and monitor it. The analysis of activities on the host is done at very fine granularity to determine precisely which processes and users are performing malicious activities on the operating system.
2. **Application-** Application-based IDS monitor the events transpiring within an application. This IDS detects attacks by analyzing the application's log files. Application-based IDSs are likely to have a fine-grained view of suspicious activity in the application by interfacing with an application directly and having significant application knowledge.
3. IDS can analyze these events using,
4. **Signature Detection-** Signature-based IDS centers around the usage of expert system to identify the intrusions based on a predetermined knowledge base. It can be used to detect each known attack if properly programmed. This technique is an effective method used in commercial products for detecting attacks [5].
5. **Anomaly Detection**-Anomaly-based IDS finds an attack by identifying the anomalous (i.e. unusual) behavior on a host or a network. The functionality of anomaly based IDS is based on the logic that some attackers behave differently than normal users and hence the attacks can be easily detected by the systems that identify these differences. These systems may generate an overwhelming number of false alarms since the variation of normal user and network behavior can vary haphazardly. Anomaly-based IDS can be used to detect the never-before-seen attacks [5].
6. Three types of attacks detected and reported by IDSs are,
   - Scanning Attacks
   - Denial of Service (DOS) Attacks
   - Penetration Attacks

II. LITERATURE STUDY

Wenke Lee ET. al.(2000) [10] has first tried to mine the system audit data to study consistent use full patter of program and user behavior. They have also used the set of relevant system features presented in the patterns to compute inductively learned classifiers that can recognize anomalies and known intrusions. In order to make the classifier an effective model they should have a sufficient audit data for training and a set of predictive system features. To guide the audit data and feature selection they have proposed the association rule and frequent episodes from the audit data, which is used in classification model. They have incorporated domain knowledge into these basic algorithms using the axis and reference attributes.

Tao Peng et. al.(2006)[11] have considered DARPA 2000 data set for Intrusion Detection Scenario to train and test the NIDS. To achieve this it has been implemented with the architecture of the data mining-based network intrusion detection system in real time. This framework is a distributed architecture consists of sensor, data preprocessor, extractors of features and detectors. To improve the efficiency they have adopted a novel FP-tree structure and FP-growth mining methods based on the FP-tree without candidate generation. Apriority candidate generation algorithm has been integrated into FP-growth method .FP-growth adopts a divide-and-conquer strategy that compresses the database representing frequent item into a frequent-pattern tree, and proceeds mining of the FP-tree. The method is highly compressed and frequent item set generation is integrated so repeated scanning of the item sets is not necessary. As they have adopted FP-growth for feature extraction the resource consuming and efficiency are satisfied.

Anazida Zainal et al. (2008) [12] in this paper has discussed the Efficiency is one of the major issues in intrusion detection. Inefficiency is often attributed to high overhead and this is caused by several reasons. The purpose of the paper is to address the issue of continuous detection by introducing traffic monitoring mechanism. In traffic monitoring, a new recognition paradigm is proposed in which it minimizes unnecessary recognition. Therefore, the purpose of traffic monitoring is two-folds; to reduce amount of data to be recognized and to avoid unnecessary recognition. For this Adaptive Neural Fuzzy Inference System and Linear Genetic Programming to form ensemble classifiers that shows a small improvement using the ensemble approach for DoS and R2L classes (attacks).

Jorge Blasco et al. (2010)[13] in this paper has studied that one of the central areas in network intrusion detection is how to build effective systems that are able to distinguish normal from intrusive traffic. To avoid the blind use of GP, it provides the search by means of a fitness function based on recent advances on IDS evaluation. For the experimental work use of a well-known dataset (i.e. KDD- 99) that has become a standard to compare research although its drawbacks. Results clearly show that an intelligent use of GP provides better accuracy and also compare the Hit rate and False Rate to detect the number of attacks.

G. Zhai et al. (2010)[14] has discussed that ID3 algorithm was a classic classification of data mining. It always selected the attribute with many values. The attribute with many values wasn't the correct one, it would created fault alarm and omission alarm. To this fault, an improved decision tree algorithm was proposed. The decision tree was created after the data collected classified correctly. With the help of using Decision tree algorithm it shows the maximum attacks and also increases the alert level after modified the decision tree.

Naveen N C et.al.(2010) [15] Has analyzed that designing the IDS for real time has become more challenging. Whenever anew thread is occurred a new knowledge map has to be built, to achieve this they have used SLFN (Single-Hidden Layer Feed Forward Neural Network). SLFN can detect attack faster compared to other methods. As a learning technique, SLFN demonstrated good potential in resolving Regression and Classification problems. Finally they have concluded that IDS using soft computing technique may prevent time consuming trials of other algorithm.

D. Md. Farid, N. Harbi and M. Z. Rahman(2010)[16], concerns Naive Bayesian classifier and ID3 algorithm. Author also talks some problems that are present in the existing one, such as handling continuous attribute, missing attribute values and treducing noise in training data. This approach solve above problems and achieves good detections rate and low false positives and also eliminates redundant attributes from training data set. This model used Knowledge Discovery Data Mining (KDD) CUP 99 dataset for experiment .

Renuka et. al.(2011) [17] has proposed an Artificial Neural network based NIDS by using a concept of ensemble binary classification and multi-boosting. Using these two concepts simultaneously it efficiently detects the attack with the low false alarm rate even at the high traffic. With the use of dynamic multi-boosting and database storage the time taken to detect the attack has been decreased efficiently

Ahmed Youssef et al. (2011)[18] has studied that Intrusion detection has become a critical component of network administration due to the vast number of attacks persistently threaten our computers. Traditional intrusion detection systems are limited and do not provide a complete solution For the problem. However, in many cases, they fail to detect malicious behaviors (false negative) or they fire alarms when nothing wrong in the network (false positive). For this combination of Data Mining Techniques and Network behavior analysis

were applied and overcome the limitations of traditional Intrusion Detection System.

Mohd. Junedul Haque et al. (2011)[19] in this paper has said that the Intrusion Detection system is an active and driving secure technology to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a network. The main part of Intrusion Detection Systems (IDSs) is to produce huge volumes of alarms. The interesting alarms are always mixed with unwanted, non-interesting and duplicate alarms. For this Data mining algorithm, K means clustering, Distributed IDS are applied to improve the detection rate and decrease the false alarm rate.

Hesham et.al.(2012)[20] has developed intrusion detection system using Bayesian probability because they wanted to improve the accuracy of the R2L attack. Used Bayesian method to classify the data accordingly. They have achieved better result than Chou's PhD result, where Chou has achieved a DR of 69.82% for the R2L. But the author has achieved better result for R2L attack with a DR of85.35% by using features like Count, Srv count and Srv_diff_host_rate with a threshold value 0.6. But the CR considerably low then Chou because they have used a low threshold value which reduces the accuracy of detection of normal record but increases DR for R2L attack.

N. S. Chandolikar, V. D. Nandavadekar (2012)[21], use J48 decision tree classifier. The author suggested many approaches for their evaluation like Root Mean Squared Error (RMSE), Mean Absolute Error (MAE), Root Relative Squared Error and Kappa statistics measures. The KDD Cup 99 data set is used for their verification. In this approach the search space is divided into rectangle region.

Chitrakar, Chuanhe (2012) [22] discussed the SVM classification and k-medoids clustering. By using k-medoids clustering similar data instances are grouped and the resulting clusters are classified by using SVM classifiers. This approach safeguard from all the attacks like Dos, probe, U2R, R2L. This approach yields high accuracy rate but it takes more time when the dataset is very large.

S.A.Joshi et al. (2013) [23] has presented that with the tremendous growth in information technology, network security is one of the challenging issue and so as Intrusion Detection system (IDS). The traditional IDS are unable to manage various newly arising attacks. To overcome this type of problem Data Mining techniques, Feature Selection, Multi boosting were applied. With data mining, it is easy to identify valid, useful and understandable pattern in large volume of data. Features are selected using binary classifiers for more accuracy in each type of attack. Multi boosting is used to reduce both the variance and bias. Thus the efficiency and accuracy of Intrusion Detection system are increased and security of network so is also enhanced.

S. Devaraju et al. (2013)[24] has discussed about the security purpose in information system. To deal with the problems of networks different classifiers are used to detect the different kinds of attacks. In this, the performance of intrusion detection with various neural network classifiers is compared. In this proposed research there are five types of classifiers used. They are Feed Forward Neural Network (FFNN), Elman Neural Network (ENN), Generalized Regression Neural Network (GRNN), Probabilistic Neural Network (PNN) and Radial Basis Neural Network (RBNN). Finally it is clear that Probabilistic Neural Network has better accuracy than rest of other neural networks

Rowayda A. Sadek et.al. (2013)[25] proposed a new hybrid algorithm NNIV-RS(Neural Network with Indicator Variable using Rough Set for attribute reduction)algorithm is used to reduce the amount of computer resources like memory and CPU time required to detect the attack. In this approach feature reduction is done by using Rough Set Theory. Indicator Variable is used to represent the data set in more efficient way. Network packet classification has been achieved by Neural Network; neural network consist of a collection of preprocessing elements that are highly interconnected and transform a set of input to a set of desired outputs. With this hybrid approach they have achieved detection rate of96.7% with false alarm rate of 3%.

Ahmed et.al.(2013)[26] in this paper intrusion detection system is papered with PSO-Descriptive-HNB is used. This is the combination of Particle Swarm Optimization (PSO) and Information Entropy Minimization (IEM) descriptive method with the Hidden Naïve Bays (HNB) classifier. Experiment is conducted on NSL-KDD data set. This proposed network IDS leads to high detection accuracy(98.2%) and speed up the time to 0.18sec after reducing the number of features from 41 to 11.

Yogitha et.al. (2013)[27] have proposed intrusion detection system using Support Vector Machine (SVM). Verification is done by conducting experiments on NSL-KDD Cup'99data set which is improver version of KDD Cup'99 dataset. By using this NSL-KDD Cup'99 data set they have reduced extensive time required to build SVM model by performing proper pre-processing on data set. In this classification is done by using SVM. By doing proper kernel selection attack detection rate is increased and false positive rate (FPT) is decreased. In this proposed work author has used Gaussian Radial Basis Function.

Sahilpreet Singh, Meenakshi Bansa(2013)[28], have proposed a paper suggested the Multilayer Perceptron feed forward neural network and use back propagation algorithm for detecting the intrusion on the network. This approach classify the attacks in an efficient way and deliver high accuracy with low error rate. The author use NSL KDD dataset and WEKA machine learning tool.

Ankita ET. Al(2014).[29] in this paper IDS is built using ensemble technique: Bagging and Boosting. They have implemented classification using SVM and Decision tree with both ensemble techniques. They have applied both techniques individually to the different classifier and results are compared.

G. V. Nadianmai and M. Hemalatha (2014)[30] in this paper the author point out four concerns which are found in an existing one like Classification of Data, High Level of Human Interaction, Lack of Labeled Data, and Effectiveness of Distributed Denial of Service (DoS) attack. The author suggested the EDADT algorithm, Hybrid IDS model, Semi-Supervised Approach and Varying HOPE RAA algorithm for solving the above stated problems. In this an enhanced data adapted decision tree algorithm is used to effectively classify the data into normal and attack without any classification. The algorithm SNORT and anomaly based approaches are being used to reduce the workload of network administrator. The frequently occurred data are classified by hybrid IDS pre-defined rules. The issue related to belling the unlabeled data is solved using Semi-Supervised approach where with the small amount of labeled data, the large amount of unlabeled data can be labeled. The author practice varying clock drift for explaining the Distributed Denial of Service Attack. This varying clock drift in network based applications makes it difficult for the intruder to access the port that has been used by the legitimate client .

Ayei ET. al.(2015) [31] has enhanced efficiency of intrusion detection by proposing a hybrid technique using both misuse and anomaly detection approaches. This is achieved by combining features of J48,Boyer Moore and K-NN algorithms. The HYBRITQ-4 performs well against four different attacks with high detection rate and low false positive rate. The experimental results have shown on different iteration.

Jaina Patel, Krunal Panchal (2015)[32] in this paper the author integrates both type of detection techniques. The irregularity data was identified by SNORT. Anomaly based IDS use both “k-means and CART” CART (Classification and Regression Trees) for classifying normal and abnormal activities in the network. The author evaluates the data from KDD Cup Dataset. The proposed assemblage is familiarized to maximize the effectiveness in identifying attacks and achieve high accuracy rate as well as low false alarm rate. The approach CART proceeds not as much of time to form decision tree than the earlier one.

Chong eik loo etc (2016)[33] has designed to sense an abnormal traffic patterns by collecting an information of normal traffic pattern. In this approach obtain maximum energy because there is no way for sharing information from neighboring nodes. Every node on the network has an individual IDS. The anomaly based approach is used to model the distribution of training points by consuming clustering algorithm which is based on a fixed width. In this model the detection rate have been increased and the false positive rate will be In this method each node has independent IDS so it leads to high configuration rate.

III. PROPOSED METHODOLOGY

The Brain storm optimization (BSO) algorithm is a new and promising swarm intelligence algorithm, which simulates the human brainstorming process. Human being is the most intelligent creature in this world. Intuitively, optimization algorithm inspired by human being creative problem solving process should be superior to the optimization algorithms inspired by collective behavior of insects like ants, bee, *etc*. In this paper, brain storm optimization algorithm is to be introduced, which was inspired by the human brainstorming process. In this research work BSO algorithm will be implemented for intrusion detection.
Here, the performance metric of accuracy has been analyzed through the various methods and it has been presented graphically.

Table I- Accuracy of the proposed method

Method	DoS	R2L	Probe	U2R
TANN	90.94	80.53	94.89	60
BPNN	80.35	89.12	89.12	25.58
FC-ANN	96.5	93.1	47.96	82.99
FBSO (proposed)	97.14	93.46	94.8	89.34

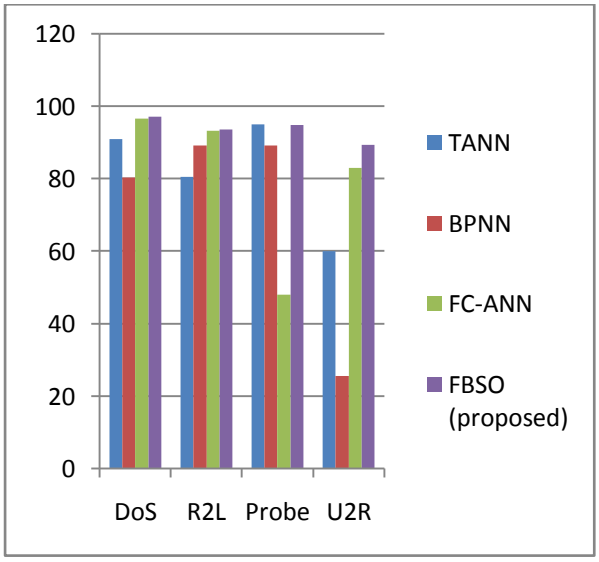

Fig.3. Graphical Representation of accuracy of proposed method

IV. CONCLUSION

The main objective of this paper is to provide an overview of the necessity and utility of intrusion detection system on embedded network. The IDS is becoming essential for day today security for network users**.** The proposed Brain Storm Optimization (BSO) used the acquired network structure as an IDS model to classify the security attacks. The achieved accuracy of embedded network is high compared to other Intrusion detection methods. From the results it is concluded that the BSO is a suitable method to prevent the security attacks on embedded networks.

REFERENCES

[1]. Maqbool BB, Bashir U, Chahcoo M. "Intrusion Detection and Prevention System: Issues andChallenges. International Journal of Computer Applications. 2013; 76.17.
[2]. Mukherjee, Biswanath L, Heberlein T, Levitt KN.Network intrusion detection. IEEE network. 1994;8(3): 26-41.
[3]. Corinne Lawrence- "IPS – The Future of Intrusion Detection"- University of Auckland - 26th October 2004.
[4]. Karthikeyan .K.R and A. Indra- "Intrusion Detection Tools and Techniques a Survey"
[5]. "Intrusion Detection and Intrusion Prevention"-Ed Sale VP of Security Pivot Group, LLC.
[6]. Proctor, Paul E. The Practical Intrusion Detection Handbook.
[7]. Bace, Rebecca. "An Introduction to Intrusion Detection and Assessment: for System and Network Security Management."
[8]. J.P. Anderson, Computer Security Threat Monitoring and Surveillance, James P. Anderson Co., Fort Washington, Pa. 1980.
[9]. Karthikeyan .K.R and A. Indra- "Intrusion Detection Tools and Techniques a Survey"
[10]. Wenke Lee ,Salvatore J. Stolfo "Adaptive Intrusion Detection: aData Mining Approach" 2000
[11]. Tao Peng, Wanli Zuo "Data Mining for Network Intrusion Detection System in Real Time" IJCSNS International Journal ofComputer Science and Network Security, VOL.6 No.2B, February2006
[12]. Anazida Zainal, Mohd Aizaini Maarof and Siti Mariyam Shamsuddin "Data Reduction and Ensemble Classifiers in Intrusion Detection" in 2008 IEEE.
[13]. Jorge Blasco, Agustin Orfila, Arturo Ribagorda "Improving Network Intrusion Detection by Means of Domain-Aware Genetic Programming" DOI 10.1109/ARES.2010.53 in IEEE 2010.
[14]. Guangqun Zhai, Chunyan Liu "Research and Improvement on ID3 Algorithm in Intrusion Detection System" in 2010 IEEE
[15]. Naveen N C, Dr. R Srinivasan , Dr. S Natarajan "A UnifiedApproach for Real Time Intrusion Detection Using Intelligent DataMining Techniques" 2011, IJCA Special Issue 2011
[16]. D. Md. Farid, N. Harbi and M. Z. Rahman,"Combining naive bayes and decision tree for adaptive intrusion detection", International Journal of Network Security & Its Applications (IJNSA), April 2010,vol. 2, no. 2.
[17]. Renuka Devi Thanasekarn "A Robust and Efficient Real TimeNetwork Intrusion Detection System Using Artificial NeuralNetwork In Data Mining" 2011 International Journal of Information Technology Convergence and Services(IJITCS) Vol. 1, No. 4, 2011
[18]. Ahmed Youssef and Ahmed Emam "Network Intrusion Detection using Data Mining and Behavior Analysis" International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 6, Dec 2011
[19]. Mohd. Junedul Haque, Khalid.W. Magld, Nisar Hundewale "An Intelligent Approach for Intrusion Detection Based on Data Mining Techniques" in 2012 IEEE
[20]. Hesham Altwaijry , Saeed Algarny "Bayesian based intrusiondetection system" 2012 Journal of King Saud University 2012
[21]. N.S.Chandolikar and V.D. Nandavadekar, "Efficient algorithm for intrusion attack classification by analyzing KDD Cup 99", Wireless and Optical Communications Networks (WOCN), 2012 Ninth International Conference on ISSN :2151-7681, (2012) September 20-22, pp. 1 - 5.
[22]. Chitrakar R, Chuanhe H, Clustering Anomaly based Intrusion Detection using Hybrid Learning Approach of combining k-Medoids and Naïve Bayes Classification, In Proceedings of 8th IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2012, p1-5.
[23]. S.A.Joshi, Varsha S.Pimprale "Network Intrusion Detection System (NIDS) based on Data Mining" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 1, January 2013
[24]. S. Devaraju, S .Ramakrishnan "Detection of Accuracy for Intrusion Detection System using Neural Network Classifier" International Journal of Emerging Technology and Advanced Engineering(ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
[25]. Rowayda A. Sadek, M. Sami Soliman and Hagar S. Elsayed"Effective Anomaly Intrusion Detection System based on NeuralNetwork with Indicator Variable and Rough set Reduction" IJC

Iinternational Journal of Computer Science Issue, Vol,10, Issue 6, No 2, 2013
[26]. Ahmed A. Elngar, Dowlat A. El A. Mohamed and Fayed F. M.Ghaleb "A Real-Time Anomaly Network Intrusion DetectionSystem with High Accuracy" 2013 Inf. Sci. Lett. 2, No. 2, 49-56(2013)
[27]. Yogita B. Bhavasar, Kalyani C. Waghmare "Intrusion DetectionSystem Using Data Mining Technique: Support Vector Machine"2013 International Journal of Emerging Technology and AdvanceEngineering volume 3, Issue 3, March 2013
[28]. Sahilpreet Singh Meenakshi Bansa ,"Improvement of Intrusion Detection Systemin Data Mining using Neural Network",IJARCSSE, September 2013,Volume 3, Issue 9
[29]. Sivaranjani S, Mr. Ravi Pathak, Vaidehi.V "Network Intrusion Detection using Data Mining Technique" 2014 International Journal of Advanced Research in Computer Engineering &Technology (IJARCET)Volume 3 Issue 6, June 2014
[30]. Nadiammai G. V, Hemalathain M,—Effective approach toward Intrusion Detection System using data mining techniques,Cairo University, Elsevier,Egyptian Informatics Journal, 2014, pp. 37-50
[31]. Ayei E. Ibor , Gregory Epiphaniou "A Hybrid MitigationTechnique for Malicious Network Traffic based on ActiveResponse" 2015 International Journal of Security and itsApplication vol 9, No. 4(2015), pp 63-80.
[32]. Jaina Patel, Krunal Panchal "Effective Intrusion Detection System using Data Mining Technique", JETIRJune 2015, Volume 2, Issue 6
[33]. Chong Eik Loo, Mun Yong Ng, Christopher
[34]. Leckie, Marimuthu Palaniswami,Intrusion Detection for Routing Attacks in Sensor Networks., International Journal of Distributed Sensor Networks, 2016, pp.313-332.
[35]. P. Garcı´a-Teodoro, J. Dı´az-Verdejo, G. Macia´-Ferna´ndez, E. Va´zquez, "Anomaly-based network intrusion detection: Techniques,systems and challenges".
[36]. Bharanidharan Shanmugam and Norbik Bashah Idris, "Hybrid Intrusion Detection Systems (HIDS) using Fuzzy Logic".

Author Profile

Mr.B.Suresh has completed his B.Sc., M.Sc., M.Phil., and Pursing Ph.D., from Erode Arts and Science College (Autonomous), Erode. Affiliated to Bharathiar University. He has published more than 10 articles in National Journals, International Journals, and conference Proceedings. Presently he is serving as Assistant professor in the Department of ECS, VLB Janakiammal College of Arts and Science College (Autonomous), Coimbatore. His research interests are Microprocessors, Embedded systems and IoT.

Dr.M.Venkatachalam has completed his B.Sc., M.Sc., M.Phil., and Ph.D., degrees from Bharathiar University. He has published more than 100 articles in National Journals, International Journals, and conference Proceedings. Presently he is serving as Associate professor and Head in the Department of Electronics, Erode Arts and Science College (Autonomous), Erode. He has served as principal investigators for many funded projects and guided many scholars leading to the award of Ph.D. His research interests are Thin Film Technology, Microprocessors, Embedded systems and IoT.