AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Artificial Intelligent Based Technique in Intrusion Detection System: A Review

[1]S.N. Suhana, [2] A.B. Rohani, [3]S. Norrozila, [4]A.N. Sukinah, [5]Y. Azliza

[1,4,5] Faculty of Computer, Media and Technology Management, TATI University College, Jalan Panchor, Teluk Kalong, 24000 Kemaman, Terengganu, MALAYSIA
[2,3] Faculty of Computer System & Software Engineering, Universiti Malaysia Pahang, 263000 Gambang, Kuantan, Pahang, MALAYSIA

ARTICLE INFO

Article history:
Received 23 December 2013
Received in revised form 25 February 2014
Accepted 26 February 2014
Available online 5 April 2014

Keywords:
Intrusion Detection System, KDD Cup (1999), Artificial Intelligent

ABSTRACT

Electric commerce and the recent online consumer boom have forced a change in the basic computer security design for systems on a shared network. Systems are now designed with more flexibility and less barrier security. Furthermore, as computers become more financially available to the masses, they also become increasingly consumer-oriented. Intrusion detection system is the whole process that audits, tracks, identifies and detects the unauthorized accesses or abnormal phenomena, actions and events in the system. The ideal of Intrusion Detection System will efficiently and effectively classify network traffic between benign and belligerent. The scope of this review will encompass core methods of artificial intelligent. The research contributions in each field are summarized, allow defining existing research challenges. The findings of this review should provide useful insights into the current IDS and be a good source for anyone who is interested in the application of IDS in artificial intelligent approach or related fields.

To Cite This Article: S.N. Suhana, A.B. Rohani, S. Norrozila, A.N. Sukinah, Y. Azliza., Artificial Intelligent Based Technique in Intrusion Detection System: A Review. ***Aust. J. Basic & Appl. Sci.,*** *8(4): 68-74, 2014*

INTRODUCTION

Internet has been the most useful technology of the modern times which helps us not only in our daily lives, but also our personal and professional lives developments. Internet is undoubtedly the most crucial technology of the modern world, the useful application has not only made our lives easier than ever before but it also plays a very important role in the future developments. The global communication has become a matter of just the finger tips of the users. The internet has brought about the various different, innovative communication means like the emailing, chatting, and the voice conversation system over the internet. These systems have not only made the communication easy but also the daily lives interactions following the business of people living on the other sides of the world. The other blessings of the internet include the umpteen resources of all over the net and also the entertainment via the games, websites, and media access which was never so easy before.

In Malaysia, there is an estimated of over1.7 billion Internet users globally, consequently estimated that consumers spent more than over $2.8 billion on online shopping worldwide in 2010. The Internet has shifted key financial and personal information to the hands of Internet users at home, as more and more commerce are transacted online by this group of Internet users. Those data may now be kept in personal computers or even mobile phones instead of large data centers owned by corporations. As a result, securing online transactions has become more complex and challenging to secure information especially contained in large data center (Network Security Portal, 2009). While e-commerce in Malaysia has yet to see the level of acceptance seen in the US or Europe, local Internet users should not be oblivious to Internet threats. Today, Internet users face Internet threats in the form of crimeware. The malicious software stealthily distributed by cyber criminals with the purpose of secretly extracting information and gaining money from Internet users. Crimeware may take the form of viruses, worms, Trojans, Botnets or other malicious programs. In addition, cyber crime allows perpetrators to hide behind the anonymity of the Internet, making it difficult for law enforcers to prosecute them.More over, according to a cyber security report released by (Symantec, 2009), nearly 10,512,000 identities are stolen every year, averaging one identity theft every three seconds. The seriousness of the situation becomes apparent when one compares this rate to crime rates in some of the largest cities in the world. New York City sees a crime once every three and a half minutes and one crime in every two and a half minutes in Tokyo.

Generally, IDS serve the role of forming the last line of defense in the overall protection scheme of a computer system. IDS is useful in detecting successful breaches of security, monitoring attempts to compromise

Corresponding Author: S.N. Suhana**,** Faculty of Computer, Media and Technology Management, TATI University College Jalan Panchor, Teluk Kalong, 24000 Kemaman, Terengganu.

security, and providing important information for timely countermeasures. Most organizations are not aware of the different types of attacks they experience on a daily basis against their systems. In literature, many IDS have been developed implementing artificial intelligent based techniques. This paper is to provide a review of intrusion detection system and various AI techniques in intrusion detection system in the academic research.

2. Literature Review:

Intrusion detection has been an active topic for about two decades, starting in 1980 with the publication of John Anderson (1980), "Computer Security Threat Monitoring and Surveillance". His paper classifies six categories of intrusive activities and how these activities might be detected. Intrusion Detection System attempts to detect intrusions, which are defined to be unauthorized uses, misuses, or abuses of computer systems by either authorized users or external perpetrators. Particularly, IDS plays a vital role in detecting various kinds of attacks, valuable tool for the defense in depth of computer networks and to resist external attacks. Aim of IDS is to provide a wall of defense to confront the attacks of computer systems on Internet. IDSs can be used on detecting in difference types of malicious network communications and computer systems usage, whereas the conventional firewall can not perform this task. These recommendations led to the development of two approaches, anomaly detection and misuse detection.

Anomaly Detection:

The idea of anomaly detection is to build a normal activity profile for a system. Anomalous activities that are not intrusive are flagged as intrusive, though they are false positives. Actual intrusive activities that go undetected are called false negatives. This is a serious issue, and is far more serious than the problem of false positives (Mukkamala *et al*., 2005). Anomalies or outliers are aberrant observations whose characteristics deviate significantly from the majority of the data or any events that significantly deviate from normal activity are considered to be suspicious. The main advantage with anomaly intrusion algorithms is that they can detect new forms of attacks, because these new intrusions will probably deviate from the normal behavior (Denning, 1987). Most of the commercial and freeware IDS tools are signature based. Such tools can only detect known attacks previously described by their corresponding signatures. The signature database should be maintained and updated periodically and manually for new attacks. For this reason, many data mining and machine learning algorithms are developed to discover new attacks that are not described in the training labeled data (Bouzida *et al*., 2004). Many intrusion detection approaches have been proposed which include statistical (Denning, 1987), machine learning (Lane, 2000), data mining (Lee, 1999) and immunological inspired techniques (Gao *et al*., 2006).

Misuse Detection:

The idea of misuse detection is to represent attacks in the form of a pattern or a siazqgnature so that the same attack can be detected and prevented in the future. These systems can detect many or all known attack patterns, but they are of little use for detecting naïve attack methods (Mukkamala *et al*., 2005). Pattern-matching solutions primarily use misuse detection. They employ a library of signatures of misuse, which are used to match against network traffic. The weaknesses of these systems are: variants, false positives, false negatives, and data overload. Since they rely on signatures, a new variant of an attack can be created to evade detection. Additionally, the signatures themselves can create false positives if they are not written correctly, or if the nature of the attack is difficult to isolate from normal traffic characteristics (Liston, 2004). Earlier studies have utilized a rule-based approach for intrusion detection, but had a difficulty in identifying new attack or attacks that had no previously describe patterns (Ilgun, 1993).

In general, IDS deals with huge amount of data which contains irrelevant and redundant features causing slow training and testing process, higher resource consumption as well as poor detection rate. Since the amount of audit data that an IDS needs to examine is very large even for a small network, classification by hand is impossible. Analysis is difficult even with computer assistance because extraneous features can make it harder to detect suspicious behavior patterns (Lee, 1999). Complex relationships exist between the features, which are practically impossible for humans to discover. IDS must therefore reduce the amount of data to be processed. This is extremely important if real-time detection is desired. Reduction can occur in one of several ways. Data that are not considered useful can be filtered, leaving only the potentially interesting data. Data can be grouped or clustered to reveal hidden patterns. By storing the characteristics of the clusters instead of the individual data, overhead can be significantly reduced. Finally, some data sources can be eliminated using feature selection.

KDD Cup (1999):

KDD Cup (1999) data was used for the Third International Knowledge Discovery and Data Mining Tools Competition, which was held in conjunction with the Fifth International Conference on Knowledge Discovery and Data Mining. Dataset of features from network packets classified into non-attack and four attack categories. The data are labeled as attack or normal, and furthermore are labeled with an attack type that can be grouped

into four broad categories of attacks. The database contained a wide variety of intrusions simulated in a military network environment. The KDD Cup 1999 provided both training dataset and test dataset. The test dataset included some specific attacks that did not appear in the training dataset to make the task more difficult and realistic. Some intrusion experts suggested that most novel attacks are variants of known attacks, and the signature of known attacks can be sufficient to catch novel variants. The datasets contained 24 training attack types, with additional 14 types in the test data only. The KDD Cup 1999 contained 4,898,431 and 311,029 records in the training set and test set, respectively. Attacks in the data sets are divided into four main categories:

i) DOS (Denial of Service): such as ping of death attack and syn flood

ii) U2R (User to Root): such as eject attack; unauthorized access to root privileges). unauthorized access to local superuser (root) privileges, e.g., various buffer overflow attacks

iii) R2L (Remote to local): such as guest attack; unauthorized access from a remote machine unauthorized access from a remote machine, e.g.guess_passwd

iv) PROBING: such as port scanning attack. surveillance and other probing) surveillance and other probing, e.g., port scanning.

The KDD Cup 1999 data set contained 41 various quantitative and qualitative features. Each TCP connection has 41 features with a label which specifies the status of a connection as either being normal, or a specific attack type. There are 38 numeric features and 3 symbolic features, falling into the following four categories:

i) Basic features: 9 basic features were used to describe each individual TCP Connection, basic features to every network connection like duration of connection, service requested, and bytes transferred between source and destination machine etc.

ii) Content features: 13 domain knowledge related features were used to indicate suspicious behavior having no sequential patterns in the network traffic, llike logged in flag, number of failed logins, hot indicators, etc.

iii) Time-based traffic features: 9 features were used to summarize the connections in the past 2 s that had the same destination host or the same service as the current connection. Time-based traffic were collected by observing various connections in "two-second" time window with respect to current connection, such as SYN error rates, Rejection rates, number of different services requested etc

iv) Host-based traffic features: 10 features were constructed using a window of 100 connections to the same host instead of a time window, because slow scan attacks may occupy a much larger time interval than 2 s., based on the past 100 connections similar to the one under consideration.

Each record was marked with a value of classification attribute, which only had two values: normal record or DDoS attack There were 9,775 records in training data with 1,928 normal records and 7,847 DoS attacks. DoS records had one of five types: Neptune, *smurf*, pod, teardrop and back attack. There were 10,952 records in testing data with 2,251 normal records and 6,184 DoS records respectively. Five new attack types just appeared in tested data not in training data. There were totally 334 of such new attacks: *mailbomb*, *land*, *proceetable*, *warezmaster* and apache attacks. These new attacks were used to find weather the system could detect new attacks.

3. Artificial Intelligent Techniques In Intrusion Detection System:

Ponce (2004) has listed many advantages of using AI based techniques over other conventional approach. The major advantages include Flexibility (vs. threshold definition of conventional technique); Adaptability (vs. specific rules of conventional technique); Pattern recognition (and detection of new patterns); Fast computing (faster than humans, actually) and Learning abilities. Many authors (Novikov *et al*., 2006; Mukkamala & Sung, 2003) have divided AI based techniques into different classes. The major classes include the following:

A) Decision Tree Based Technique:

Decision trees are powerful and popular tools for classification and prediction. A decision tree is a tree that has three main components: nodes, arcs and leaves. Each node is labeled with a feature attribute which is most informative among the attributes not yet considered in the path from the root, each arc out of a node is labeled with a feature value for the node's feature and each leaf is labeled with a category or class. A decision tree can then be used to classify a data point by starting at the root of the tree and moving through it until a leaf node is reached. The leaf node would then provide the classification of the data point (Kumar & Sachdeva, 2010). Levin (2000) has created a set of locally optimal decision trees from which optimal subset of trees is selected for predicting new cases. 10% of KDD Cups database is used for training and testing. Data is randomly sampled from the entire training data set. Multi-class detection approach is used to detect different attack categories in the KDD data set. Levin has tried to classify the data into five different classes: Normal, Probing, DOS, U2R, and R2L. The final trees give very high detection rates for all classes including the R2L in the entire training data set.

B) Machine Learning Technique:

Machine learning can be defined as the ability of a computer programs to learn and enhance the performance on a set of tasks over time. Machine learning techniques focus on building a system model that enhances its performance based on previous results. Alternatively it can be said that system based upon machine learning have ability to manipulate execution strategy based upon new inputs (Kumar *et al*., 2010) The machine learning has been successfully implemented in intrusion detection. Major machine learning techniques include the following:

C) Particle Swarm Optimization:

Particle Swarm Optimization is robust and has been proven theoretically and empirically to be able to search the optimum solution or near-optimal solution to a complex problem. However, if current optimal position is discovered by certain particle, the other particle will draw close to the optimal position rapidly in the process of running. If this optimal position is local optimal point, particle population will not research in the solution space. Thus, PSO is easy to sink into local optimized solution that is to say, premature phenomena is appeared. Many scholars resolve problems above by combination with particle swarm optimization and genetic algorithms or selection inertia weight. Berhart & Shi (1998) put forward the strategy of linear decreasing inertia weight, which is applied in particle swarm optimization algorithm. Although this strategy improves the performance of particle swarm optimization, it is related with iteration times of PSO and cannot really reflect the algorithms' characteristics of complex and nonlinear in the process of running

D) Neural Network:

The Neural Network learns to predict the behavior of the various users and daemons in the system. If properly designed and implemented, NN have the potential to address many of the problems encountered by rule-based approaches. The main advantage of NN is their tolerance to imprecise data and uncertain information and their ability to infer solutions from data without having prior knowledge of the regularities in the data. This in combination with their ability to generalize from learned data has made them an appropriate approach to IDS (Kumar *et al*., 2010). NN can be used in following ways:

i) Unsupervised model: Cunningham & Lippmann (2000) of MIT Lincoln Laboratory have conducted a number of tests employing Neural Networks to misuse detection. The system was searching for attack-specific keywords in the network traffic. A Multi Layer Perceptron has been used for detection UNIX host attacks, and attacks to obtain root-privilege on a server. The system was trying to detect the presence of an attack by classifying the inputs into 2 outputs (normal and attack). The system was able to detect 85% of attacks, 17 out of 20 attacks were identified. The main achievement of this system was its ability to detect old as well as new attacks. The new attacks were not included in the training data. They have used DARPA intrusion detection evaluation dataset.

ii) Supervised model: Self-Organizing Maps (SOM) has been proved to be effective in novelty detection, automated clustering, and visual organization (Ypma & Duin, 1998). Bivens *et al*. (2002) have detected the intrusions based on network user behavior. They have analyzed the user behavior based on time window using neural networks. After supervised learning of neural network, the network data has been classified and clustered by using Self Organizing Map (SOM) neural network in different time intervals. These clusters are used to detect the attack in network. The approach has used DRAPA TCP dump data for training of neural network. Kayacik *et al*. (2003) have utilized KDD Cups data set for the experiments. They have created three layer of employment: First, individual SOM are associated with each basic TCP feature. This provides a concise summary of the interesting properties of each basic feature, as derived over a suitable temporal horizon. Second layer integrates the views provided by the first level SOM into a single view of the problem. At this point, they have used training set labels associated with each pattern to label the respective best matching unit in the second layer. Third, final layer is built for those neurons, which win for both attack and normal behaviors. These results in third layer SOMs being associated with specific neurons in the second layer. Moreover, the hierarchical nature of the architecture means that the first layer may be trained in parallel and the third layer SOMs are only trained over a small fraction of the data set.

iii) Hybrid neural network model: Many researchers have tried to combine Multi-Layer Perceptron model (MLP) and Self-Organizing Map (SOM) for intrusion detection (Kumar *et al*., 2010). They have attempted to create an Intrusion Detection System using MLP and SOM for misuse detection (Novikov *et al*., 2006). They have used a feed-forward network with back-propagation learning, which contained 4 fully connected layers, 9 input nodes and 2 output nodes (normal and attack). The network has been trained for a certain number of attacks. The network has succeeded in identifying attacks it was trained for.

E) Support Vector Machine:

Support vector machine (Vapnik, 1995; Cortes & Vapnik, 1995) is a new kind of machine learning algorithm proposed recently which is based on structural risk minimization of statistical learning theory. Many

researchers verified that SVM performed well in intrusion detection classification (Hansung *et al*., 2005; Mukkamala *et al*., 2002; Dong *et al*., 2005). However, when applying standard SVM on high dimension and large-scale dataset, such as network connection dataset, it often suffers memory storage and time consuming problem because a standard SVM solver will solve a dual quadratic optimization problem (Lee & Stolfo, 1999; Mukkamala *et al*., 2000). Decreasing the dimension of training samples by feature selection or attribution reduction method is benefit to help alleviate this problem. Comparing with traditional ANN, SVR possesses prominent advantages such as excellent properties in learning limited samples, good generalization ability, etc. SVR is originally developed for solving classification problems and later extended to solve regression problems, and exhibits good learning performance (Steve, 1998). However, there exists a problem in the practical application of SVR. This problem is how to select some of SVR parameters so that the performance of SVR can be brought into the best.

Mukkamala *et al*. (2002) compare performance of ANN and SVMs in intrusion detection. They have empirically proved that features selected with help of SVM leads to similar results as use of full feature set. This reduction in number of features improves computational effort. Chen *et al*. (2005) have also proved that SVM is superior to NN. The superior performance of SVMs over ANNs is due to the following three reasons:

i) SVMs implement the structural risk minimization principle which minimizes an upper bound for the generalization error rather than minimizing the training error. However,
ANNs implement the empirical risk minimization principle, which might lead to worse generalization than SVM.

ii) An NN may not converge to global solutions due to its inherent algorithm design. In contrast, finding solutions in SVMs is equivalent to solving a linearly constrained quadratic programming problem, which leads to a global optimal solution.

iii) In choosing parameters, SVMs are less complex than ANNs. The parameters that must be determined in SVMs are the kernel bandwidth and the margin C. However, in ANNs, the number of hidden layers, number of hidden nodes, transfer functions and so on must be determined. Improper parameter selection might cause the over-fitting problem.

Tarun Ambwani (2003) reports his multi-class SVM to intrusion detection. The standard method for N-class SVM is one-versus-rest which constructs N SVMs. Ambwani uses one-versus-one method which constructs all possible n*(n-1)/2 two-class SVMs. The detection rate of Ambwani's one-versus-one multi-class SVM seems good, but he did not present the time cost of his methods, as well as the problem of confusions of multi-hyper-planes. For one-versus-rest or one-versus-one SVMs, many hyper-planes are constructed, but in these methods, the hyper-planes do not promise a perfect separation. Therefore, Takahashi & Abe (2003) propose decision-tree-based SVMs. In their method, in training, a decision tree in which each node presents a decision hyper-plane which separates one or some classes from others are constructed by top-down ways. By this method, when training is finished, the feature space is divided by N-1 hyper-planes and there are no unclassifiable regions. DT SVMs are also efficient to deal with confusions. Unfortunately, it is hard to control the classification error of decision tree, which is performance of one node will influence the whole sub-tree below it.

F) Rough Set Theory:

Rough Set Theory is the most widely used baseline technique of single classifier approach on intrusion detection. In addition, it has also been considered recently for model comparisons. Before training, the step of feature or variable selection may be considered. The process of feature selection identifies which features are more discriminative than the others. This has the benefit of generally improving system performance by eliminating irrelevant and redundant features (Chih Fong *et al*., 2009).

Many analyses have been done to come out with significant rules. Since the generated rules possible to have in large number of rules, it is important to know whether all rules played a role in the classification process. Indranil Bose (2006) has suggested that, to find the most significant rules for each sample, the rules are sorted according to the value of their support. The generated rules do not differ much in terms of length and thus support is used as the criterion for ranking the rules. Subsequent analysis is the evaluation of the rules length to obtain testing accuracy. Typically, rules of less length ascend to a higher overall testing accuracy. This indicates that the dataset led to the formation of a smaller number of rules, can correctly recognize the problem. The overall testing accuracy is highest when the training sample is reduced to 10% from the original sample. Then, the experiment of changing the parameters associated with the testing procedure is implemented. The experiment is conducted using four factors; balance of sample, a ratio of training to testing sample size, testing sample size and training sample. The experiment resultant that there was no significant effect of changing the balance of the sample, training to testing sample size, training sample size and testing sample size on testing accuracy across all samples. The best classification result is obtained and the comparisons are made with two other statistical approaches; logistic regression and discriminant analysis. The reported results reveal that Rough Set Theory method generally performed better than the others in terms of classification accuracy on training and testing samples.

Conclusion:

This paper has reviewed the essential of Intrusion Detection System. Consequently the more accurate detection is needed in real time IDS. The representation of Intrusion Detection System data understanding is important to probe the high resultant classification. An attempt has been made in this study to review the IDS data representation and presenting various artificial intelligent techniques applied in Intrusion Detection System.

ACKNOWLEDGEMENT

Authors would like to thank to *Faculty of Computer, Media and Technology Management (FKMPT)*, TATI University College and *Faculty of Computer System and Software Engineering*, Universiti Malaysia Pahang for the support in making this study a success.

REFERENCES

Ambwani, T., 2003. Multi class Support Vector Machine Implementation to Intrusion Detection. *Proc. IEEE International Joint Conference on Neural Networks,* pp: 2300-2305.

Anderson, J.P., 1980. Computer Security Threat Monitoring and Surveillance, tech. report, James P. Anderson Co., Fort Washington.

Bivens, A., P. Chandrika, R. Smith, B. Szymanski, 2002. Network-based intrusion detection using neural networks. In: Proceeding of ANNIE 2002 conference, ASME Press, pp: 10-13.

Bose, I., 2006. Deciding The Financial Health Of Dot-Coms Using Rough Sets. *School of Business, University of Hong Kong*.

Bouzida, Y., F. Cuppens, N. Cuppens-Boulahia, S. Gombault, 2004. Efficient Intrusion Detection Using Principal Component Analysis. *3ème Conférence sur la Sécurité et Architectures Réseaux (SAR)*, La Londe, France.

Chen, W.H., S.H. Hsu, H.P. Shen, 2005. Application of SVM and ANN for intrusion detection. Comput Oper Res., 32: 2617-2634.

Chih-Fong, T.a., H.b. Yu-Feng, L.c. Chia-Ying, L.d. Wei-Yang, 2009. Intrusion Detection by Machine Learning: A review, a Department of Information Management, National Central University, Taiwan b Department of Information Management, National Sun Yat-Sen University, Taiwan c Department of Accounting and Information Technology, National Chung Cheng University, Taiwan d Department of Computer Science and Information Engineering, National Chung Cheng University, Taiwan.

Cortes, C., V. Vapnik, 1995. Support vector networks. *Machine Learning*, 20(3): 273-297.

Cunningham, R., R. Lippmann, 2000. Detecting computer attackers: recognizing patterns of malicious stealthy behavior. MIT Lincoln Laboratory-presentation to CERIAS.

Cunningham, R., R. Lippmann, 2000. Improving intrusion detection performance using keyword selection and neural networks. Comput Netw, 34(4): 597-603.

Denning, D.E., 1987. An intrusion-detection model. *IEEE Transactions on Software Engineering*, *vol. 13.*

Dong, S.K., N.N. Ha, S.P. Jong, 2005. Genetic algorithm to improve SVM based network intrusion detection system. *19th International Conference on Advanced Information Networking and Applications*, *Vol.2*, Taiwan, 3: 155-158.

Gao, J., H. Cheng, P.N. Tan, 2006. A Novel Framework for Incorporating Labeled Examples into Anomaly Detection. *Siam Conference on Data Mining*, Bethesda, Maryland, USA.

Hansung, L., S. Jiyoung, Daihee, Park, 2005. Intrusion Detection System Based on Multi-class SVM. *Lecture Notes in Computer Science, vol.3642*, Springer Berlin, 9: 511-519.

Ilgun, K., 1993. USTAT: A Real-Time Intrusion Detection System for UNIX. *Proceedings of the 1993 IEEE Symposium on Security and Privacy*.

Kayacik, G., N. Zincir-Heywood, M. Heywood, 2003. On the capability of an SOM based intrusion detectionsystem. In: Proceedings of the 2003 IEEE IJCNN, Portland, USA.

Kumar, G., K. Kumar, M. Sachdeva, 2010. The use of artificial intelligence based techniques for intrusion detection: a review. Artif Intell Rev., 34: 369-387. DOI 10.1007/s10462-010-9179-5.

Lane, T.D., 2000. Machine Learning techniques for the Computer Security of Anomaly Detection. vol. Ph.D.: Purdue University.

Lee, W., 1999. A data mining framework for constructing features and models for intrusion detection systems. Columbia University.

Lee, W., S. Stolfo, K. Mok, 1999. A Data Mining Framework for Building Intrusion Detection Models. *Proceedings of the IEEE Symposium on Security and Privacy*.

Lee, W., S.J. Stolfo, 1999. A data mining framework for building intrusion detection model. *Proceedings of the 1999 IEEE Symposium on Security and Privacy.Oakland*, CA:IEEE Computer Society Press, pp: 120-132.

Levin, I., 2000. KDD-99 classifier learning contest LLSoft's results overview. SIGKDD Explor, 1(2): 67-75.

Liston, K., 2004. Intrusion Detection FAQ: Can you explain traffic analysis and anomaly detection?

Mukkamala, R.K., J. Gagnon, S. Jajodia, 2000. Integrated data mining techniques with intrusion detection. *Research Advances in Database and Information Systems Security.* Kluwer Publisher, pp: 33-46.

Mukkamala, S., G. Janoski, A.H. Sung, 2002. Intrusion Detection Using Neural Networks and Support Vector Machines. *Proceedings of IEEE International Joint Conference on Neural Networks, Vol 2*, Honolulu, 5: 1702-1707.

Mukkamala, S., A.H. Sung, 2003. Artificial intelligent techniques for intrusion detection. IEEE Int Conf Syst Man Cybern.

Mukkamala, S., A.H. Sung, A. Abraham, 2005. Intrusion detection using an ensemble of intelligent paradigms. *Journal of Network and Computer Applications*, 28: 167-182.

Novikov, D., R.V. Yampolskiy, L. Reznik, 2006. Artificial intelligence approaches for intrusion detection. Systems, applications and technology conference, LISAT 2006. IEEE Long Island, 5(5): 1-8.

Ponce, 2004. Intrusion detection system with artificial intelligence. In: FIST conference-edition-1/28 Universidad Pontificia Comillas de Madrid.

Retrieved from: http://myconvergence.com.my/main/images/stories/PDF_Folder/jan2010/MyCon06_63.pdf retrieved on 2011, November 15.

Retrieved from: http://bit.ly/46kCzF, retrieved on November 16, 2010.

Retrieved from http://kdd.ics.uci.edu/databases/kddcup99/task.html, retrieved on November 15, 2010.

Shi, Y., R. Eberhart, 1998. A Modified Particle Swarm Optimizer. *IEEE World Congress on Computation Intelligence*, pp: 69-73.

Steve, R.G., 1998. Support Vector Machines for Classification and Regression. *Technical Report*, University of Southampton Press, Southampton, UK.

Takahashi, F., S. Abe, 2003. Decision-Tree-Based Multi class Support Vector Machines. *Proc. International Conference on Neural Information Processing*, 3: 1418-1422.

Vapnik, V., 1995. The Nature of Statistical Learning Theory. *Springer-Verlag Press*, New York , American

Ypma, A., R. Duin, 1998. Novelty detection using self-organizing maps. Progress in connectionist-based information systems, 2.