I.J. Computer Network and Information Security, 2014, 9, 51-57
Published Online August 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.09.07

Artificial Intrusion Detection Techniques: A Survey

Ashutosh Gupta
Department of computer science, Ambedkar Institute of Advanced Communication Technology and Research (AIACTR), New Delhi, INDIA
E-mail: ashu1294@gmail.com

Bhoopesh Singh Bhati
Assistant Professor, Ambedkar Institute of Advanced Communication Technology and Research (AIACTR), New Delhi, INDIA
E-mail: bhoopesh.cse@gmail.com

Vishal Jain
Assistant Professor, Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi, INDIA
E-Mail: vishaljain83@ymail.com

Abstract—Networking has become the most integral part of our cyber society. Everyone wants to connect themselves with each other. With the advancement of network technology, we find this most vulnerable to breach and take information and once information reaches to the wrong hands it can do terrible things. During recent years, number of attacks on networks have been increased which drew the attention of many researchers on this field. There have been many researches on intrusion detection lately. Many methods have been devised which are really very useful but they can only detect the attacks which already took place. These methods will always fail whenever there is a foreign attack which is not famous or which is new to the networking world. In order to detect new intrusions in the network, researchers have devised artificial intelligence technique for Intrusion detection prevention system. In this paper we are going to cover what types evolutionary techniques have been devised and their significance and modification.

Index Terms—Artificial Neural Network, Genetic Algorithm, Immunity, Intrusion Detection, False Alarm.

I. Introduction

Internet is the global system of interconnection of computer networks that use the standard protocol (TCP/IP) to serve several user worldwide. Internet has become one of the most integral part of an individual. With the recent advancement in network based technology and dependability of our everyday life on this technology, assuring reliable operations of network based system is very important. There has been a major increase in the attacks on networks. This became the most prominent reason for the development of Intrusion Detection System (IDS).[1] There has been many researches in this field and many techniques have been evolved over a period of time. The main aim of this paper is to review the current trends in Intrusion Detection System (IDS) and to analyze some current problems attacks is not just a probability, but it is an accepted fact.

An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an information system, almost always with the intent to do harm. Even when such attacks are self-propagating, as in the case of viruses and distributed denial-of-service attacks, they are almost always instigated by someone whose purpose is to harm an organization [2]. One of the main aim of IDS is to make sure that case of the new attack, it is able to detect the attack and report it. Once the attack is reported then the administrator will be aware and try to avoid these attacks in the future. In this way the IDS will be upgraded and it will protect the network from the known attack. Monitor, detect and respond are three basic function of the Intrusion Detection System. IDS is a very good tool to detect the attack on the network but still it cannot be trusted all alone. It requires human expert also in order to assess those alarms.

There are two main types of approaches in the Intrusion Detection System. Host based and Network-based. Host based Intrusion Detection System (HBIDS) is present on a particular computer and operates on those systems which are the potential threat to the network. It generates alarms as soon as it detects any malicious activities or any threat. These alarms are sent to the administrator of that network so that actions can be taken as soon as possible. There are different types of HIDS like Tripwire, Cisco HIDS, and Symantec ESM. Network based Intrusion detection system resides on the computer or application connected to a part on an network traffic on that segment looking for indication of ongoing or successful attack [3] [1]. Different types of NIDS are

Snort, Netprowler.

The rest of the paper is divided as follows. Section2 describes some related work on intrusion detection approaches, comparison is also being made between this section. In section 3, genetic algorithm and its use in intrusion detection is explained. Section 4 presents artificial neural network and its application in many IDS. Section 5 shows how artificial immune system is effective in detecting and defending intrusions. Comparison is also being made between three evolutionary intrusion detection systems. The conclusion is given in section 6.

A. Intrusion Detection Approaches :

There are many approaches which are proposed by many researchers. We classified these approaches into two groups Traditional approaches and Evolutionary approaches. Those approaches which do not involve any type of Artificial Intelligence (AI) are taken under Traditional approaches and those which involve AI are termed as Evolutionary algorithm.

Traditional approaches are like statistical-anomaly approaches, rule based approaches, Expert system approach, pattern recognition approach, agent based approaches etc.

Evolutionary approaches include artificial neural network approach, Genetic algorithm approach, Artificial immune system, Fuzzy Logic approach etc.

II. RELATED WORK: TRADITIONAL APPROACHES FOR INTRUSION DETECTION

A. Statistical Anomaly Intrusion Detection System

It collects statistical summaries by observing traffic that is known to benormal. This normal period of evaluation establishes a performance baseline. Once the baseline is established, the stat IDPS periodically samples network activity and, using statistical methods, compares the sampled network activity to this baseline. When the measured activity is outside the baseline parameters, exceeding what is called the clipping level, the IDPS sends an alert to the administrator.

Advantage of stat IDPS is that it can easily detect new attacks as it is always looking for anomalous activities. But these systems require a lot of CPU usage and memory as they are processing the data packets all the time. Other disadvantage of this IDS is that it may not detect some small changes or can generate the false alarm. Sorting of these false alarm will again require human expert and this leads to the consumption of time and labor. [4]

B. Signature Based Intrusion Detection System

A signature-based IDPS (sometimes called a knowledge-based IDPS or a misuse-detection IDPS) examines network traffic in search of patterns that match known signatures—that is, preconfigured, predetermined attack patterns. Signature based IDPS technology is widely used because many attacks have clear and distinct signatures, for example: (1) foot printing and fingerprinting activities use ICMP, DNS querying, and e-mail routing analysis (2) exploits use a specific attack sequence designed to take advantage of a vulnerability to gain access to a system [5].

It has many disadvantages too. It has to be updated time to time otherwise new attacks might get their way through these IDPS. It is considerably slow and also requires the memory space for processing and comparing the pattern.

C. Rule based Intrusion Detection System

This IDS is totally based on some predefined rules that are provided by the administrator. Each rule has specific operation in the system. These rules are being updated time to time so that known attacks can be detected very easily.

Besides the fact that the false alarm in this IDS is very less, there are many drawbacks in this IDS. It cannot detect many new attacks. It requires a human expert to constantly upgrade this system [6].

III. EVOLUTIONARY APPROACHES FOR INTRUSION DETECTION

This type of intrusion detection involves many Artificial Intelligence (AI) techniques. Here are some of the Evolutionary approaches using those techniques.

Table 1: Comparison between different approaches

Intrusion Detection System	**Network Based Intrusion Detection System**	**Host Based Intrusion Detection System**
Presence	Present on the computer/application connected to part of an organization's network	Present on the particular server or a system, denoted as host, and controls activity
Types of software	Snort, Cisco NIDS and Netprowler	Tripwire, Cisco HIDS and Symantec HIDS
Basis	Signature comparing	Configure and alteration
Advantages of IDS	Network operations may not get disturbed in this IDS	Detect the irregularity in the attack
Limitations of IDS	Not capable to analyze encrypted data	Requires huge memory not suitable for large traffic network
Attacks being detected	DOS,CGI, Port Scans, SHB probes Layer 3	File Integrity check, Shell Attack, FTP Scans, SQL Injections

These intrusion detection techniques are being devised because they can deal with uncertain and partially true data. The main idea of involving evolutionary algorithm is to increase the efficiency of the IDS.

There are many techniques that are devised to detect the attacks and prevention of those attacks

IV. Intrusion detection based on genetic algorithm

Genetic Algorithm can also be very helpful in IDS. Genetic Algorithms are computerized search and optimization algorithms based on the mechanics of natural genetics and natural selection. In order to understand the working GA, biological background is very important. All organisms consist of cells as their building block. In each cell, there are chromosomes which further consist of strings of DNA. A chromosome consists of genes on the blocks of DNA. Every gene encodes a particular pattern. These patterns decide the traits. During the creation of an offspring, recombination occurs and in that process genes from parents form a whole new chromosome in some way. The new created offspring can then be mutated. Mutation means that the element of DNA is modified [7]. The fitness of an organism is measured by means of success of organism in life. Genetic Algorithms are inspired by Darwinian Theory of Survival of the Fittest. Algorithm is started with a set of solution called populations. Solutions for one population are taken and used to form a new population. This is motivated by a hope that a new population will be better than the old one.

Genetic Algorithm uses the process of natural selection and crossover in which chromosome like in which chromosome like data structures are used and these chromosomes are evolved with the help of mutation and recombination processes. An evaluation function is used in order to calculate the validity of each chromosome which should be fit from the previous generation chromosome.[8] For survival and combination of chromosomes is biased towards the fittest algorithm. Fitness function is applied in order to get the fitness score and based on this score forthe crossover to create new rules or hypothesis. So each time there is a new attack, the algorithm will automatically update itself in order to detect new malicious activities. This makes the approach for better than any approach present in the field of Intrusion Detection. Genetic Algorithm is capable of evolving rules that match only attacks on the network. For more clarity, the figure 1 is also included which demonstrates the basic Genetic Algorithm process[8].In the paper of Wei Li et al [9], the rules are in the form of basic if then else form:

If {condition} then {act};

The *condition* here refers to those criteria which satisfy the attack. The *act* above describes those security policies which should be taken whenever these attacks are encountered. The basic idea behind applying GA is to detect any malicious activity as soon as possible and the actions must be taken against that attack. Whenever there is a ping attack in the network, these attacks can be detected much sooner but the actions are taken on it really late. Using this technique can also reduce response time and increase the efficiency of the IDS.

In the paper of Chetan Kumar et al [10], they have used GALIB C++ library to develop GA. Their fitness function is given by the formula of

F = a/A + b/B, where a denotes quantity of attack correctly detected out of A attacks. Similarly b denotes quantity of normal connections in the total of B attacks.

There are some advantages of GA based IDS. It is easy to module and separate from other applications. It gets better with time as it is based on experience. It is more flexible and provides friendly environment for the development and alteration of network. It is also used when there is a need to combine it with an existing solution [11]. The genetic algorithms is also being used in training the neural network for intrusion detection [12].

V. Artificial neural network based intrusion detection system

A. Introduction

The idea behind the application of soft computing techniques and particularly ANNs in implementing IDSs is to include an intelligentagent in the system that is capable of disclosing the latent patterns in abnormal and normal connection audit records, and to generalize the patterns to new (and slightly different) connection records of the same class.The results show that even a multi-layer perceptron (MLP) with a single layer of hidden neurons can generate satisfactory classification results. Because the generalization capability of the IDS is critically important, the training procedure of the neural networks is carried out using a validation method that increases the generalization capability of the final neural network.

B. Origination of Neural Network

Artificial neural network is inspired by the functioning and structure of constituents of the human brain, especially neuron. In the link [12], they have discussed about the structure of a neuron. A neuron is composed of nucleus called soma. There are long irregularly shaped filaments attached to neuron called dendrites. Dendrites behave as input channels, all inputs from other neurons arrive through the dendrites. There is another type of link attached to the soma known as Axon. Axon is electrically active and serves as an output channel. The axon terminates in the specialized contacts called synapse or synaptic junction. The synaptic junction is a very minute gap at the end of the dendritic link contains a neuro-transmitter fluid. This fluid is responsible for accelerating or retarding the accelerating charges to the soma. The size of soma is likely to be related to learning. Synapses with larger area are thought to be excitatory while those with the smaller area are believed to inhibitory. Donald Hebb suggested that “when an axon of cell A is near enough to excite a cell B and repeatedly takes part in firing it some growth process or metabolic changes take place in one or both cell such that A’s efficiency as one of the cells firing bis increased”.

The modern era of neural network research is credited with the work done by neuro-physiologist, Warren McCulloh and mathematician, Walter Pitts in 1943. Both of them wrote a paper on how neurons might work. The next major breakthrough in the fields of neural network was made by Donald Hebb in 1949. He wrote a book about the neurons in NN named as “The Organization Of Behavior”. But this research did not help many researchers to solve the arising problem in this field. After the fifteen years of McColloh and Pitt’s work, a new approach in Neural Network was introduced. This approach of perceptron not only became famous but solved many big problems of pattern recognition in NN. The perceptron was the first “practical” Artificial Neural Network. The idea of perceptron was originated from the functioning of the fly eye. Perceptron model comprises of three layers sensory unit, associative and response unit. The S unit comprises of 400 photo detectors receives input and gives binary output [13].

C. Research on Neural Network Intrusion Detection System

There have been many researches in this field. Many models have been devised using the concept of Neural Network (NN). A new approach to Intrusion Detection using ANN and fuzzy clustering. In this paper [14], the researcher used the hybridization of fuzzy clustering and existing neural network. In this model, they have used FCM to generate training datasets. In this way, they have increased the performance of ANN. They also compared FCM-ANN with BPNN and other famous proposed models. In the paper [15], researchers have proposed IDS technique which is based on Evolutionary Neural Network. ENN uses an evolutionary algorithm which not only sets the internal parameter but also designs the architecture of neural network simultaneously. The design can be prepared by knowing how many weights are required and how many hidden nodes can be used. Ghosh and other researchers have used some basic properties of neural network in order to find out intrusion like feed-forward back propagation [16].

D. Advantages of Artificial Neural-Network based Intrusion Detection System

There is a great amount of flexibility that allows room for the growth and general learning. If an element of neural network fails, it can continue without any problem by their parallel nature. In Intrusion Detection system, it gives potential to tackle the most prominent of multiple types of attacks. A neural network will make a quick analysis on the type of attacks which are regular and recognize the pattern and learn it for future. This not only increases the accuracy but also reduces manual labour and false alarm to some extent. It also makes sure that the attack once recognized cannot take place in the future. Its generalization property enables it to detect unknown attacks and variations in the known attacks. The speed is also another advantage of having neural network. Artificial Neural Network has ability to assemble patterns which has common features and classifies the attack.

VI. Artificial Neural Network Based Intrusion Detection System

The major problem in the field of Intrusion Detection is how to differentiate between the normal activity and real threat. There are many models which are capable of detecting malicious activities but they have their own shortcomings and limitations the most common approach is to define the rules and recognize the datasets and whenever it deviates from the normal behavior there will be an alarm generated for the administrator. This method requires a lot of human attention, labor, time and this IDS generates lot of false alarm.

As we all know that, many organisms especially humans have survived billions of years. These organisms are capable of adapting any circumstance. This ability of surviving in harsh environment is possible only because of the Immune System. The immune system is a system of biological structures and processes within an organism that protects against disease. To function properly, an immune system must detect a wide variety of agents, from viruses to parasitic worms, and distinguish them from the organism's own healthy tissue [17]. In computer science, artificial immune systems are a class of computationally intelligent systems inspired by the principles and processes of the vertebrate immune system [18]. The algorithm typically exploits the immune system’s characteristics of learning and memory to solve a problem.Before moving towards artificial immune system, we would like to discuss about the human immune system. An immune system has mainly four properties: detection, diversity, learning and tolerance. For human immune system, there are basically four layers: skin, pH temperature, Innate Immune System, Adaptive Immune System. There are some basic terminologies that we should know. An epitope is a recognizable characteristic of a molecule, as seen by an immune system. One of the greatest advantages of immune system is its ability to detect insiders and outsiders. Antigens are epitopes that are recognized by the immune system as outsiders. Antibodies are the part of immune system which is responsible of detecting and binding to the antigens.

First layer skin is a physical barrier which prevents any antigen to cross and enter into the human body. A pathogen is capable of entering into the system can penetrate through the skin it will meet a layer of pH temperature. Some pathogens can cross these two layers and they encounter the first immunity system that is the innate immunity system. This system has more specific response and has no memory. If the pathogen crosses all these layers, it will be taken care of by the second part of immune system which is the adaptive immune system which demonstrates responses to individual antigens [19] Inspiring from the working of immune system there has been many models of Intrusion detection based on artificial immune system. Clonal selection, Negative selection and Immune networks are some famous models of IDS. The mechanism by which self-reactive lymphocytes are removed is known as negative selection and this process is known as clonal detection. These T-cells that remains alive in this process should not react with self –antigens. Immunological tolerance is the ability of lymphocytes not to react with the self-antigens. This whole mechanism described above inspires many negative selection algorithms in the field of artificial immune. There are many negative selection algorithms in the field of artificial immune system [20].There many negative selection algorithms which are being proposed by many researchers. The first algorithm was given by many researchers. The first algorithm was given by the Forrest in the year 1994[21].

The algorithm starts with the production of asset of self strings states the normal conditions of the system. After this, the main aim is to produce a group of detectors that bind the complement of self-antigens. These detectors are also applied to new data whether it manipulated or not. Many researchers are going to increase the efficiency [23][24]. Here is some comparisons being made between few evolutionary approaches used in latest IDS table 2.

VII. Conclusion

Lot of research work has been going on Intrusion Detection System. There are many types of software available on Intrusion prevention system and intrusion detection system based on the Traditional approaches. But their performance is not too efficient as there is a greater chance of false alarm and updating is mandatory after a fixed period of time. These limitations can be avoided up to a certain level by the implication on Evolutionary based IDS (EBIDS). Whenever there is a new attack on the network, detects the anomaly and train itself to for this threat. In this way, it updates itself against new attacks.

VIII. Future work

Though EBIDS has greater advantage on the Traditional based IDS, but there are no full proof system. From the above comparative analysis, we have seen that neural network based IDS is one of the most efficient IDS in the field of Intrusion detection system. There are some limitations on ANN that can be overcome with a little bit of modification and manipulation. There can be hybridization of Genetic Algorithm and Neural Network in order to overcome the limitations of the IDS. There have been many researches on hybridization of different models. The future of IDS lies in Evolutionary Techniques.

References

[1] http://en.wikipedia.org/wiki/Internet.

[2] Michael E. Whitman, Herbert J. Mattord "Principles of Information Security" pp.

[3] Karthikeyan .K.R and A. Indra "Intrusion Detection Tools and Techniques – A Survey"International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010 pp 901-906.

[4] Michael E. Whitman, Herbert J. Mattord "Principles of Information Security" pp.

[5] http://www.sans.org/security-resources/idfaq /statistic_ids.php.

[6] Iftikar Ahmad, Azween B Abdullah, Abdullah S Alghamadi Comparative Analysis of Intrusion Detection Approaches 2012 21th International Conference on Computer Modelling and Simulation pp 586-591.

[7] S. Rajasekaran, Pai G. A. Vijayalakshmi "Neural Networks, Fuzzy Logic, and Genetic Algorithms: Synthesis and Applications" pp.

[8] Mohammad SazzadulHoque, Md. Abdul Mukit and Md. Abu NaserBikas "AN IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING GENETIC ALGORITHM" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012 pp 110-120.

[9] Wei Li, Using Genetic Algorithm for Network Intrusion Detection.

[10] AnupGoyal, Chetan Kumar (2008) GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System.

[11] S. Rajasekaran, Pai G. A. Vijayalakshmi "Neural Networks, Fuzzy Logic, and Genetic Algorithms: Synthesis and Applications" pp.

[12] http://library.thinkquest.org/C007395/tqweb/history.html.

[13] Gang Wang, Jinxing Hao,Jian Ma, Lihua Huang "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering".

[14] Sang-Jun Han and Sung-Bae Cho "Evolutionary Neural Network for Anomaly Detection Based on the Behaviour of a Program", IEEE Transaction on System, Man, and Cybernetics- Part B CYBRNETICS VOL. 36, NO. 3, JUNE 2006.

[15] Deqiang Zhou," Optimization Modeling for GM(1,1) Model Based on BP Neural Network " I. J. Computer Network and Information Security, 2012, 1, 24-30 Published Online February 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2012.01.03.

[16] http://en.wikipedia.org/wiki/Immune_system.

[17] .http://en.wikipedia.org/wiki/Artificial_immune_system.

[18] ArefEshghiShargh "Using artificial immune system on Implementation of Intrusion Detection System", 2009 Third UKSim European Symposium on Computer Modelling and Simulation.

[19] http://www.artificial-immune- systems.org/ algorithms.shtml.

[20] Susan C. Lee, David V. Heinbuch "Training a Neural-Network Based Intrusion Detector to Recognize Novel Attacks" IEEE TRANSACTION ON SYSTEM, MAN AND CYBERNETICS- PART: SYSTEMS AND HUMANS, VOL. 31, NO. 4, JULY 2001.

[21] Chung-Ming Ou, C. R. Ou "Multi-Agent Artificial Immune Systems (MAAIS) for Intrusion Detection: Abstraction from Danger Theory" Agent and Multi-Agent Systems: Technologies and Applications Lecture Notes in Computer Science Volume 5559, 2009, pp 11-19.

[22] Patricia Mostardinha, Bruno Filipe Faria, André Zúquete, FernãoVistulo de Abreu "A Negative Selection Approach to Intrusion Detection" Artificial Immune Systems

Lecture Notes in Computer Science Volume 7597, 2012, pp 178-190.

[23] Mahdi Mohammadi, Ahmad Akbari, BijanRaahemi, BabakNassersharif "A Real Time Anomaly Detection System Based on Probabilistic Artificial Immune Based Algorithm" Artificial Immune Systems Lecture Notes in Computer Science Volume 7597, 2012, pp 205-217.

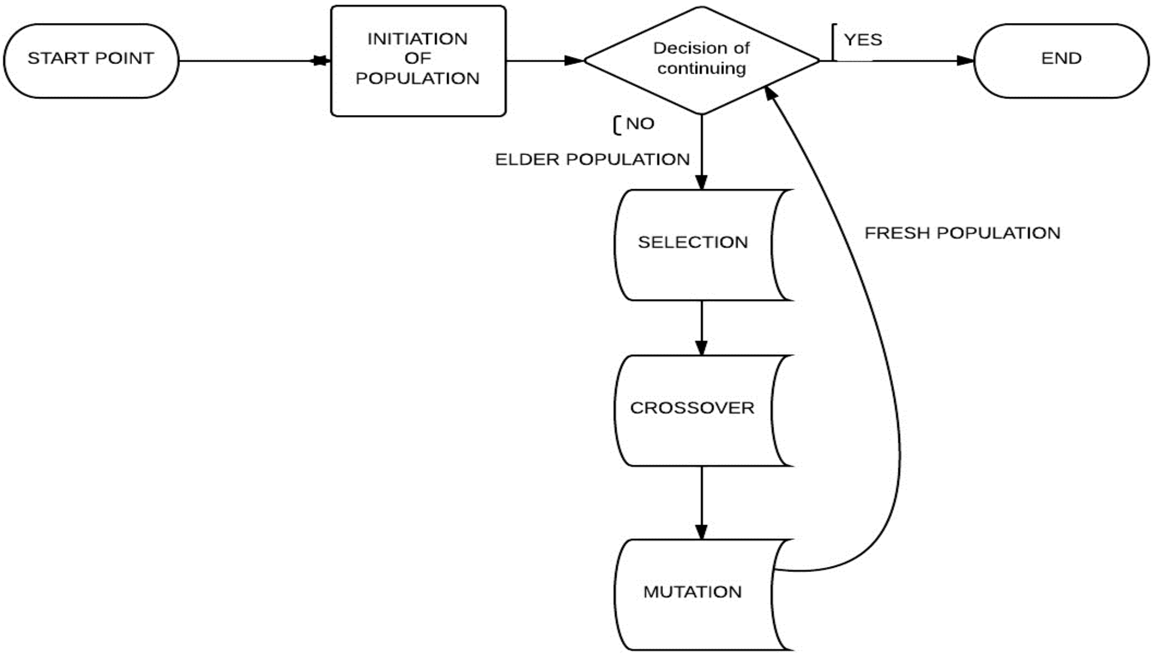

Fig. 1: Basic Genetic Algorithm Process

Table 2: Comparisons between Evolutionary Intrusion Detection Approaches

Approaches	**Artificial Neural Network**	**Artificial Immune System**	**Genetic Algorithm**
Intrusion Detection Techiques	Anomaly	Anomaly	Misuse
Input Data	Data sets, perceptron	Data sets, Sequence of Algorithms	Data sets , Fitness Function
Detecting known threats	Yes	Yes	Yes
Detecting unknown threats	Yes	Yes	No
Related paper work included in this survey	Gang Wang [13], Sang-Jun Han [14], Susan C. Lee[19]	Chung-Ming Ou[20], Patricia Mostardinha[21], Mahdi Mohammadi[22]	Md. SazzadulHoque[8], Wei Li[9], Chetan Kumar [10]
Performance of IDS	High	Moderate	Low

Author's Profile

Ashutosh Gupta, Pusruing B.Tech. degree (Computer Science and Engineering) from G.G.S.I.P. University Delhi. He published a research paper on information retrieval and semantic web in National Journal. His current research area is Multimedia Information Retrieval.

Bhoopesh Singh Bhati, Pursuing Ph.D. degree from the G.G.S.I.P. University Delhi. He has obtained M.Tech. Degree in Information Security and B. Tech. (Computer Science and Engineering) from the G.G.S.I.P. University Delhi. He is working as an Assistant Professor in the department of Computer Science and Engineering of Ambedkar Institute of Advanced Communication Technologies & Research, Govt. of NCT, Delhi-110031. He published various Research Paper in International Journals and Conferences. His current research area is Information Security.

Vishal Jain has completed his M.Tech (CSE) from USIT, Guru Gobind Sidgh Indraprastha University, Delhi and doing Ph.D from Engineering Department, Lingaya's Computer Science and University, Faridabad. Presently he is working as Assistant Professor in Bharati Vidyapeeth's Institute of Computer Applications and Management, (BVICAM), New Delhi. His research area includes Web Technology, Semantic Web and Information Retrieval. He is also associated with CSI, ISTE.

How to cite this paper: Ashutosh Gupta, Bhoopesh Singh Bhati, Vishal Jain,"Artificial Intrusion Detection Techniques: A Survey", IJCNIS, vol.6, no.9, pp.51-57, 2014. DOI: 10.5815/ijcnis.2014.09.07