International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 183-194
http://dx.doi.org/10.14257/ijsia.2015.9.6.18

New Approach to Monitoring Internet Access along with Usage of Bandwidth Using Intrusion Detection System

D. Rajagopal[1], K. Thilakavalli[2] and K. Syed Ali Fathima[3]

K.S.R College of Arts and Science[1], K.S.R College of Arts and Science for women[2], M.Kumarasamy College of Engineering[3]
sakthiraj2782007@gmail.com[1], thilaksathya2782007@gmail.com[2], safathima07@gmail.com[3]

Abstract

New Approach to observe web Access beside Usage of information measure victimization Intrusion Detection System could be a comprehensive web use observation and news utility for company networks. It takes advantage of the very fact that the majority companies give web access through proxy servers, like MS ISA Server, MS Forefront TMG, WinGate, WinRoute, MSProxy, WinProxy, EServ, Squid, Proxy Plus, and others. Whenever the user accesses several websites, transfer files or pictures, these actions were logged. The system processes these log files to supply system directors a good vary of report-building choices. It might build reports for individual users, showing the list of internet sites visited, beside elaborate classification of web activity (downloading, reading text, viewing footage, observation movies, paying attention to music, and working). This technique might produce comprehensive reports with analysis of overall information measure consumption, building easy-to-comprehend visual charts that show the areas wherever wasteful information measure consumption has eliminated. This new approach is employed to observation the web information measure employed by the user. victimization this technique will simply decide that user fill the information measure most heavily, when, and what specifically they transfer, what proportion time they pay on-line, and what knowledge transfer traffic they produce.

Keywords: *Web, Bandwidth, Download, Intrusion, Network Traffic*

1. Introduction

Network managers and directors should get on guard against all types of unauthorized network use. Intrusion Detection System observation network traffic for activity that falls inside the definition of prohibited activity for the network. When found, the Intrusion can alert directors and permit them to require corrective action, interference access to vulnerable ports, denying access to specific science addresses, or move down services wont to enable attacks, this fast-alert capability makes an Intrusion Detection System the front-line weapon within the network directors war against hackers. The planned Intrusion Detection System put in on the server that serves native hosts and users over web. There are four actors within the system monitor, user, network and computer user. User sends request to the server over the web or native space Network and Intrusion Detection System can analyze the packets received by the server. This Intrusion Detection System detects each internal and external intrusion. If it detects any intrusion then it alerts computer user.

The planned approach permits centralized monitor of Users web access prevents personal usage of company information measure, reduces the web expenses, very easy-to-use. It will begin observation user's couple of minutes once, once the installation complete, works with all trendy proxy servers, permits the generation of a good range of reports and diagrams, that show the potency of proxy server usage, and it's a task

ISSN: 1738-9976 IJSIA

computer hardware to automates the creation and delivery of reports to authorize personnel.

1.1. Advantages of the Approach

- Allows centralized observation of Users web access
- Prevents personal usage of company information measure and reduces the web Expenses
- Extremely easy-to-use; will begin observation users couple of minutes once, once the installation is complete
- Works with all trendy proxy servers and permits the generation of a nice range of reports and diagrams, that show the potency of Proxy Server usage
- Task computer hardware to automates the creation and delivery of reports to authorize personnel.

2. Intrusion Detection System

Intrusion Detection refers to the method of observation the system for unauthorized access incidents, which might be the violation of the protection policy, system use policy, or the other security standards [1]. On the opposite hand, An Intrusion Prevention System (IPS) prevents unauthorized access incidents from being prosperous. To safeguard the system from any attacks, Intrusion Detection and Prevention System (IDPS), that give an utterly machine-controlled observation service, deployed on the systems. Most of the IDPS systems log the incident on every occasion an attack on the system is that observe and notifies the administration of the system so all necessary actions will taken to avoid such incidents once more within the future. The directors of the system also can put together the IDPS to observe the violations of the tip user policies and alternative unauthorized activities.

3. Intrusion Detection System Types

3.1 Network Intrusion Detection System

It is a freelance platform, which identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection System gain access to network traffic by connecting to a network hub, network switch designed for port mirroring, or network faucet [2, 3]. A NIDS is place on a network to investigate traffic in search of unwanted or malicious events. Network traffic designed on varied layers; every layer delivers knowledge from one purpose to a different. The OSI model and transmission management protocol (TCP)/IP model show however, every layer stacks up. Inside the TCP/IP model, rock bottom link layer controls however, knowledge flows on the wire, like dominant voltages and the physical addresses of hardware, like Mandatory access Control (MAC) addresses.

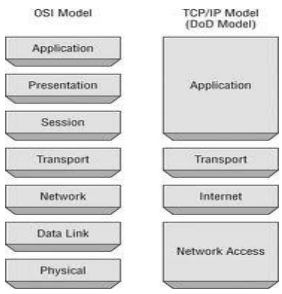

Figure 3.1. OSI and TCP/IP Models

The web layer controls address routing and contain the science stack. The transport layer controls knowledge flow and checks knowledge integrity. It includes the communications protocol and user datagram protocol (UDP). Lastly, the foremost sophisticated however most acquainted level is that the application layer, that contains the traffic employed by programs. Application layer traffic includes the online (hypertext transfer protocol [HTTP]), file transfer protocol (FTP), email, etc. Most NIDSs observe unwanted traffic at every layer; however concentrate totally on the applying layer.

Two main element sorts comprise a NIDS: appliance and software package solely. A NIDS appliance could be a piece of dedicated hardware: it is solely operated to be IDS. The Operating System (OS), software, and the network interface cards (NIC) are enclose within the appliance. The second element kind, software package solely, contains the entire IDS software package and generally the OS; but the user provides the hardware. Software-only NIDSs are usually more cost-effective than appliance-based NIDS because of they are doing not give the hardware; but, a lot of configuration is need, and hardware compatibility problems could arise.

3.1.1. Advantages of Network Based IDS

- Monitor network for port scans.
- Monitor network for malicious activity on known ports such as http port 80.
- Identify varied varieties of spoofing attacks.
- Does not impact network performance.
- Increased tamper resistant.
- Operating systems independent.

3.1.2 Drawbacks of Network Based IDS

- Packets lost on flooded networks.
- Reassemble packets incorrectly.
- No understanding of O/S specific application protocols like SMB.
- No understanding of obsolete network protocols.
- Does not handle encrypted data.

3.2. Host-Based Intrusion Detection System

It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, secret files, capability databases, Access management lists etc.) and alternative host activities and state [4]. Whereas a NIDS watches the traffic on a network phase, HIDS watches the activities of a selected host. A common open-source HIDS system is OSSEC, named as a contraction of Open Source Security.

OSSEC can monitor the Windows registry, the file system of the pc, generated logs, and more, looking for suspicious behavior. As with a NIDS, an alert are going to be generated by any suspicious activity on the host and also the administrator will set these results of the alert. If a method is trying to modify the documents on the most internet server, for instance, OSSEC will kill the process, shut the account that launched it, and contact to the computer user. It is a remarkably versatile and spectacular system.

Much like a NIDS, the position of HIDS software package must arrange carefully. The user doesn't need to receive an alert on every occasion a file is reaching on a digital computer. The system has fastidiously to put together and the monitored behaviors cropped to on eliminate false alarms and make sure the true security problems are noticed and alerted properly.

3.2.1 Advantages of Host Based IDS

- Monitor events native to a host, and might observe prosperous or failure of attacks that cannot be seen by a network-based IDS.
- Operate in the setting during which network traffic encrypted.
- Unaffected by switched networks and is independent of topology.
- Monitor system specific activities like file access, user access, etc.
- Provide thorough data gathered via logs and audit; for instance, Kernel logs know who the user is.
- No extra hardware is required to implement Host based IDS solution.
- When Host-based IDSs operate on OS audit trails, they will facilitate observe attacks that involve software package integrity breaches.

3.2.2. Drawbacks of Host Based IDS

- Host based IDS are tougher to manage, as data should be designed and managed for each host singly.
- Host based IDS's network blind and cannot detect a network scans or other such surveillance that targets entire network.
- If the host is compromised, collected log by Host based IDS can be subverted.
- Disabled by bound denial-of-service attacks.
- Uses operating system audit trails as an information source. The number of information is large and might need extra native storage on the system.
- Inflict performance deficiency on monitored host.

3.3. Stack-Based Intrusion Detection System

This type of system consists of an evolution to the HIDS systems. The packets examined as they are going through the TCP/IP stack and, therefore, it is not necessary for them to work with the network interface in promiscuous mode. This reality makes its implementation to be dependent on the Operating System [5].

This can be latest IDS technology and varies dramatically from vendor to vendor. Stack Based IDS works by integration closely with the TCP/IP stack, allowing packets to be watch as they traverse their way up the OSI Layers. observation the packets during this means permits the IDS to drag the packets from the stack. To be complete Stack- Based ID ought to watch each incoming and outgoing network traffic on a system. By monitoring network packets destined just for a simple host, the principle is to create the IDS have sufficiently low overhead so each system on the network will run Stack-Based IDS.

4. Intrusion Detection Techniques

4.1. Statistical Anomaly-Based IDS

A statistical anomaly-based IDS determines traditional network activity like what type of bandwidth is mostly used, what protocols are used, what ports and devices usually connect to each other- and alert the administrator or user once traffic is detected that is abnormal(not normal) [6]. The anomaly-based detection model detects the attacks based on the profiles. The profiles contain the patters or the traditional behavior during which the system is used. The profiles supported specific users, networks, or the applications. They are making by monitoring the system use over a period, known as the evaluation period. This model compares the present activities with the profiles to get the abnormal activity in progress, which regularly is an attack. Since the system use and also the network use do not seem to be not static and always contain some variation over time, the

profile should additionally modify consequently. Therefore, once the creation of the profiles in the evaluation period, an IDPS changes the profiles over time. The samples of the profiles mentioned below. A user profile contains an email activity of 5%. Once the IDPS victimization anomaly-based detection model senses that the e-mail activity on the system is over 5%, it will consider about it an attack. Over the past few weeks, on average a user performs that open, read, and write operations on the file system for 2% of the time. Once the IDPS detects a growth within the file access operations, it reports an attack incident. The advantage of the anomaly-based detection model is that it is able to detect even unknown attacks by comparision the present abnormal events with something that is considering traditional. Further, this model also can be more efficient than the signature-based model given that there are a large range of signatures to compare inside the signature-based detection model. On the other hand, the attack incidents that anomaly-based model produces don't seem to be terribly specific and it takes some efforts by the administrator to pin - purpose the basis of the attack. Additionally this model subject to a "slow attack". In this type of attack, the attacker first finds out the threshold between the normal and abnormal activities. The attacker then would slowly attack the system making sure that the activities during the attack do not reach the threshold which results into the anomaly-based detection model not detect the attack.

4.1.1 Advantages of Anomaly Based IDS

- Identify any potential attack.
- Identify attacks that have not seen before, or close variants to antecedently well-known attacks.

4.1.2. Drawbacks of Anomaly Based IDS

- Normal will amendment over time, introducing the requirement for periodic on-line preparation of the behavior profile, result either in inaccessibility of the intrusion detection system or in extra false alarms.
- Current implementations give high false alarms.
- Requires experience to work out what triggered an alarm.

4.2. Signature-Based IDS

Signature based IDS monitor's packets within the Network and compares with pre-configured and pre-determined attack patterns called signatures. The difficulty is that there will be lag between the new threat discovered and Signature being applied in IDS for detecting the threat. Throughout this lag time, IDS are going to be unable to spot the threat. The signature refers to the pattern during which a antecedently well-known attack was performed. The signature-based detection methodology is that the method of comparison the present events with the signatures. The signature-based detection model produces terribly specific attack event reports as oppose to the anomaly-based detection model. The disadvantage of a signature-based detection model is its inability to detect new unknown attacks since the system does not have any signature entry within the system for the new attacks.

4.2.1. Benefits of Signature Based IDS

- Provides terribly low false alarms as compare to Heuristic based IDS.
- Provides detail contextual analysis providing steps for preventive or corrective actions.

4.2.2. Drawbacks of Signature Based IDS

- It is tough to assemble data concerning well-known attacks and keeping up-to-date with new vulnerabilities.
- Signatures and corrective recommendations are generalized; so it makes it tougher to grasp them.
- Knowledge concerning attacks is extremely centered, keen about the operating system, version, platform, and application.
- Signature/Pattern based IDS are more popular and commercially used than Heuristic/Anomaly detection based IDS. Major vendors such as ISS offer network based and host based signature detection.

5. Network Bandwidth

Network bandwidth refers to the amount of knowledge being transmitted across a network at any given purpose in time. Network bandwidth will decrease if devices that change networked communications fail. Network bandwidth might be forced by each hardware and software package limitations. Optimizing the out there Network information measure could be a primary responsibility of network administrators.

6. Proposed System Result

The result of the Intrusion Detection Expert System (IDES) has become a regular in intrusion detection systems. Many current systems are based in partly on IDES prototype technology, The Next –Generation Intrusion Detection Expert System (NIDES) is the comprehensive enhancement to IDES. NIDES is a real-time intrusion detection application which integrates a statistical analysis -based anomaly detector and a rule-based misuse detection system. The combination gives the flexibility to observe penetrations from internal and external attacks. NIDES additionally includes a comprehensive program that allows access to any or all the applications capabilities, similarly as a context –sensitive facilitate system.

While NIDES is considered the present progressive during a combined anomaly and misuse detection system, the applying retains the problem possessed by all similar models in detection cooperative attacks, long-term penetration situations and virus propagation. Another potential disadvantages is that NIDES retains the reliance on the system's audit record for input. Future expansions of the rulebase and the development of profiles of entities aside from users ought to scale back the potential vulnerabilities that don't seem to be adequately addressed by the present system.

One of the main challenges to attempting implement and validate a new intrusion detection methodology, is to assess it and compare its performance therewith of alternative out there approaches. It is noticeable that this task is not restricted to A-NIDS, however is additionally applicable to NIDS (and even to IDS sometimes) generally. The requirement for test-beds that provide robust and reliable metrics to quantify NIDS has been prompt, for instance, by the National Institute for Standards and Technology (NIST). An advantage of assessment in real environments is that the traffic is sufficiently realistic; however, this approach subject to: (a) the risk of potential attacks, and (b) the possible interruption of the system operation due to simulated attacks. On the other hand, the evaluation of NIDS methodologies in experimental environments involves the generation of synthetic traffic as well as background traffic representing legal users, that is much from being a trivial endeavor.

Several studies have examined the use of the two varieties of testing methodologies. This can be summarized within the following contributions to dealing traffic databases: - In 1998, DARPA (Defense Advanced Research Project Agency) started a programme at the MIT Lincoln Labs with the aim of providing an entire and realistic benchmarking

environment for IDS. The agency project was reviewed in 1999, and also the resulting 1999 DARPA/Lincoln Laboratory intrusion detection evaluation dataset (IDEVAL) became a widely used benchmarking tool by which synthetic network traffic was generated. Additionally, in 2001, DARPA, in collaboration with other institutions, started the LARIAT (Lincoln Adaptable Realtime Assurance Test-bed) programme. Unfortunately, LARIAT is restricted to US military environments and to some academic organizations under special circumstances. Many contributions within the literature have raised questions on the accuracy of the agency simulations. In this respect, many efforts have been made to obtain new traffic databases.

However, all these proposals quickly became obsolete, as the traffic was out-of-date compared with that of current networks. Furthermore, the specifications of the corresponding datasets are not described in detail. Another key issue about traffic databases is the confidentiality of the data. Some researchers propose anonymity through IP address masquerading, which has the advantage of real traffic while avoiding the problem of ciphering. This can be honest approach, but sometimes the masquerading process is carried out without any consideration of the information kept in each IP address, workload or URI, which could be useful for some NIDS systems. Therefore, it would be good practice to change the IP addresses in such a way that the relations between the real and the faked addresses are univocal. The same applies to other masqueraded information: user-ID, URI, etc. Usually, these basic rules do not seem to be obeyed, and the anonym databases become useless. Other network traffic related studies deal with the problem of standardizing the acquisition and use of real traffic for validating NIDS environments. During this respect, that contributes some proposals on a general methodology to amass and organize traffic datasets, to outline AN analysis framework to check the performance of anomaly-based NIDS. The significant try created up to now in NIDS assessment proof of its importance. However, it remains an open issue and a big challenge.

A new methodology that would achieve more accuracy than the existing six classification patterns (Gaussian Mixture, Radial Basis Function, Binary Tree Classifier, SOM, ART and LAMASTAR),called Hierarchical Gaussian Mixture Model[HMM] for IDM. Development of host-based anomaly intrusion detection, focusing on system call based HMM training. This was later enhanced with the inclusion of data pre-processing for recognizing and eliminating redundant sub sequences of system calls, resulting in less number of HMM sub models. Experimental results on three public databases showed that training cost can be reduced by 50% without affecting the intrusion detection performance. False alarm rate is higher yet reasonable compared to the batch training method with a 58% data reduction. An anomaly detection system comprising of detection modules for detecting anomalies in each layer. The anomaly detection results of the neighbor node(s) is taken by the current node and its result in turn is sent to the neighbor node(s).Experimental results revealed increased detection rate and reduced false alarm positives, compared to other methods.

The new framework builds the patterns of network services over datasets labeled by the services. With the built patterns, the framework detects, attacks in the datasets. This approach is independent of attack-free training datasets, but assumes that each network service has its own pattern for normal activities.

The biometrics-based intrusion detector model to provide a light-weight and self-contained module for detection user identities misuse. System-calls and network traffic monitoring systems ought to be combined to the present detector to achieve the best solutions. The proposed a technique to detect anomalies at all layers of a network stack in a sensor network, segregating the service at various levels. Physical layer intrusion is detected by using RSSI values of neighbors (dependant on background noise, weather conditions etc). Targeting MAC layer will work for schedule based and sleep/wake-up based MAC protocols whereas IASN protocol is geared toward the routing layer.

Experiments show that IASN is used for supply started routing protocols, table driven routing protocols and data dissemination mechanisms like directed diffusion. The probability of detection increases linearly with the amount of nodes running IASN. Nodes guard each other from masquerade at application layer. Depending on the resource availability, any combination of the above methods can be employed, as they are independent of one another. All technique are energy efficient as they have very low false positive rates(except RSSI and round trip time) and low overhead.

Combining multiple independent data sources and studying combined traditional intrusion attack and anomaly intrusion, the anomaly intrusion traffic detection provided the statistical wavelet based detection mechanism. The properties like attack length, packet count, packet rate, and dominant protocol kind match with the two data sets, as is showed by attack structure. At lean and significant traffic situations, the demand capability of the server was determined to administer higher clarity of anomaly intrusion detection though server period of time. Analysis of many traffic anomaly properties that is not possible victimization ancient intrusion measurements is performed by a brand new model that used anomaly intrusion attack measurements.

Small businesses appear to be the foremost common targets of attacks. Traditional measures in understanding and detecting of anomaly intrusion is no more reliable given the current trends of attacking, using spoofed address sources. Windows Host Anomaly Detection System, which is used as a supplement for other security mechanisms under windows. It can only detect intrusions which invoke an anomaly sequence by programs. One of the general situations such as an unauthenticated use of normal programs cannot be detected.

The Statistical anomaly detection technology called that HIDE with hierarchical multitier multi-observation window system to monitor network traffic parameters simultaneously, using a real-time probability distribution function(PDF) for each parameter, collected during the observation window. The similarity measurements of measured PDF and reference PDF are combined into an anomaly status vector classified by a neural network. This technique detects that attacks and soft faults with traffic anomaly intensity as low as 3 to 5 percent of typical background traffic intensity, thereby generating an early warning.

The anomaly based mostly intrusion detection system for mobile networks, supported simulation results of quality profiles for enhancing ABID in mobile wireless networks. If the quality behavior of users has not been accurately found, the choice of specific values for key parameters, like sequence length and cluster size is absurd. One potential strategy for enhancing the characterization of users and addressing construct drift (keeping official up-to-date), is to take care of a window of the fresh determined sequences (analogous to the exponential weighted moving average) which will then be wont to update the coaching patterns sporadically and, thus scale back the false positives.

An intrusion detection algorithm and its architecture (two layered, global central layer and a local layer, together performing data collection, analysis and response), based on data mining and useful in real time for network security, By filtering out the known traffic behavior (intrusive and normal) the IDS focuses on analysis on unknown data thereby reducing false alarm rates. The model supported contiguous professional selection rule ways observe most anomalies, unsuccessful match does not imply AN abnormity, as traditional rules might not cowl all traditional data. Detection rates in this is not commendable but it has vast future scope for improvement.

In recent literature, anomaly detection through a Bayesian Support Vector Machine is found as interesting machine learning model for anomaly detection. Use of a SVM with one-class to detect the system anomalies at their early stage is studied along with drift output classification probabilities. Experimentally, absence of failure training data under one-class SVM leads to quick detection of unknown anomalies. Initially dividing the training data into multiple unrelated lower dimensional models, the test data will be

evaluated on each model separately thereby revealing outliers in different capacities (as is used to evaluate the posterior class probabilities in Bayesian framework).

7. Results of the Various Algorithms

The experimental results that have obtained with the assorted algorithms. the assorted rules designed and whose results are bestowed the Brute-Force algorithm, the Karp-Rabin rule, the Boyer-Moore rule and also the Knuth-Morris-Pratt rule.

The results of the running time of these algorithms vary the input size, where the input is the words. The number of patterns to be matched remains the same. The running time (in milliseconds) for the various algorithms is recorded within the following table.

Input Size	Running Time (in milliseconds)			
	Brute-Force	Karp-Rabin	Knuth-Morris-Pratt	Boyer-Moore
20000	15	15	17	15
60000	46	45	46	40
100000	74	73	79	68
140000	102	102	108	102
180000	129	132	139	119
200000	144	144	159	133

The graph for the above tabulated data

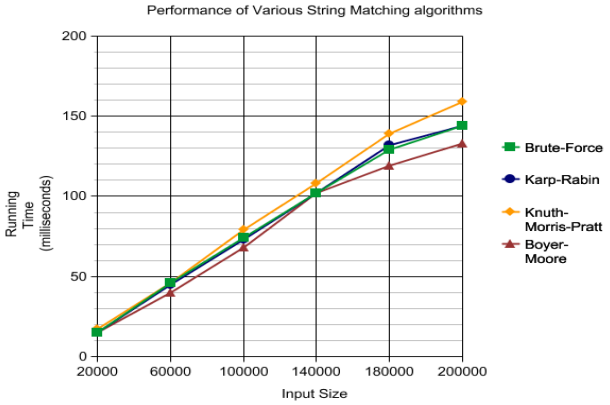

Figure 7.1. Performance between the Algorithms

From the table and the graph, there is no trend within the performance between the algorithms. Solely that KMP performs the worst and Boyer-Moore performs the simplest.

8. Conclusion

The extension of the model with additional attributes can help to unearth further mistakes. The analysis of statistical properties of router configurations appears to be a promising approach to help operators in detecting mistakes. Unlike most of the current research, which use only one agent per engine for detection of various attacks, the proposed system is constructed by several agents in a single engine. The NIDS will broaden its read on completely different behaviors of the network traffic by every of the agents with its own strength on capturing a form of network behavior. Firewall policy rules are one in every of most significant part of network security system. It plays the very important role in management of any organization's network and its security infrastructure.

Thus the management of policy rule could be a vital task for the network security. There are many tools and techniques won't to perform anomaly detection and rule editing by using given set of existing policy rules. However, one in every of the idea and so its limitation is that firewall and its rules are set to be static and so while not a capability to replicate the network behavior determined by firewall.

References

[1] Namita Shrivastava, Vineet Richariya, "Ant Colony Optimization with Classification Algorithms used for Intrusion Detection", "IJCEM International Journal of Computational Engineering & Management", Vol. 15 Issue 1, January 2012,PP:54-63.
[2] NITIN D. SHELOKAR1 and S.A. LADHAKE, "Network Intrusion detection using correlation functional dependency", "Oriental Journal of Computer Science & Technology", Vol. 3(1), 185-188 (2010).
[3] V.Sivakumar, T.Yoganandh, R.Mohan Das, "Preventing Network From Intrusive Attack Using Artificial Neural Networks", "International Journal of Engineering Research and Applications (IJERA)", Vol. 2, Issue 2,Mar-Apr 2012, pp.370-373.
[4] Utkarsh Dixit, Shivali Gupta and Om Pal, "Speedy Signature Based Intrusion Detection System Using Finite State Machine and Hashing Techniques", "International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, September 2012,pp: 387-391.
[5] Miss. M. R. Yadav, Prof. P. B. Kumbharkar, "Intrusion Detection System with Supervised Learning Algorithms", "International Journal of Advanced Research in Computer Science and Software Engineering", Volume 4, Issue 4, April 2014, PP 305-310.
[6] Manju Khari, Manas Gaur, Yatin Tuteja, "Meticulous Study of Firewall Using Security Detection Tools", "International Journal of Computer Applications & Information Technology", Vol. II, Issue I, January 2013, pp 1-9.

Authors

D. Rajagopal, he has completed his Bachelor of Computer Science degree and completed his Master of Computer Applications degree in Periyar University in the year 2003 and 2006 respectively. He completed his Master of Philosophy in PRIST University in the year of 2012. He has 3 Years and 10 Months Experience in the field of Software Developing and 4 Years and 6 months Experience in the field of Teaching. He published three International Journal papers and a National Conference paper. He delivered more than 10 seminar & training programs for different Academic Institutions. His research area of Interest is Computer Networks (Wireless & Wired), Image Processing, Mobile Computing, Data Mining, Software Programming (OOPS). Currently he is working as an Assistant professor in the Department of Computer Science in K.S.Rangasamy College of Arts and Science (Autonomous), Tiruchengode, Namakkal Dt, Tamilnadu, India.

K. Thilakavalli, she has completed her Bachelor of Physics degree in Bharathiar University in the year of 2006. She completed her Master of Computer Applications degree in Anna University in the year 2009. She completed her Master of Philosophy in PRIST University in the year of 2010. She has 5 Years 6 months experience in the field of Teaching. She published three International Journal papers, three International Conference papers, and two National Conference papers. Her research area of Interest is Image Processing, Computer Networks (Wireless & Wired), Mobile Computing, Data Mining.

Currently she is working as an Assistant Professor in the Department of Computer Applications in K.S.R College of Arts and Science for women, Tiruchengode, Namakkal Dt, Tamilnadu, India.

K. Syed Ali Fathima, she has completed her Bachelor of Engineering in Syed Ammal Engineering College, Anna University in the year 2009, and she completed her Master of Engineering degree in Kalasalingam University in the year of 2012. She has 3 Years experience in the field of teaching. Currently she is working as an Assistant Professor in the Department of Computer Science and Engineering in M.Kumarasamy College of Engineering. Her research area of interest is Image processing, Computer networks, Mobile computing, Data mining.