International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-2, Issue-4, 2018.
www.ijirtm.com *ISSN: 2581-3404 (Online)*

Improve the Rate of Malicious Attack Detection using Neural Network and Classification Technique

Vivek Kirar[1], Prof. Jitendra Mishra[2]
[1]M. Tech Scholar, Department of EC, PCST, Bhopal (India)
[2]Head & Professor, Department of EC, PCST, Bhopal (India)
[1]kirar.vivek@gmail.com, [2]jitendra.mishra260@gmail.com

ABSTRACT
Malware is basically malicious software or programs which are a major challenge or major threats, for the computer and different computer applications in the field of IT and cyber security. Traditional anti-viral packages and their upgrades are typically released only after the malware's key characteristics have been identified through infection. The most common detection method is the signature based detection that makes the core of every commercial anti-virus program. In this paper we improved the rate of malware detection using neural network classifier and compare with the other technique i.e. support vector machines, and show that the support vector machine classifier result better than the neural network classifier.

Keywords: Malware detection, Neural network, Support vector machine, Classification techniques, Supervised learning.

INTRODUCTION
Malware is defined as computer software that has been explicitly designed to harm computers or networks. In the past, malware creators were motivated mainly by fame or glory. Most current malware, however, is economically motivated. Commercial anti-malware solutions rely on a signature database for detection. An example of a signature is a sequence of bytes that is always present within a malicious executable and within the files already infected by that malware. In order to determine a file signature for a new malicious executable and to devise a suitable solution for it, specialists must wait until the new malicious executable has damaged several computers or networks.

This approach has proved to be effective when the threats are known beforehand. Malware writers use code obfuscation techniques [5] to hide the actual behavior of their malicious creations. Examples of these obfuscation algorithms include garbage insertion, which consists on adding sequences which do not modify the behavior of the program, code reordering, which changes the order of program instructions and variable Renaming, which replaces a variable identifier with another one [9].

Data-mining-based approaches rely on datasets that include several characteristic features for of both malicious samples and benign software to build classification tools that detect malware in the wild. The first to introduce the idea of applying data-mining models to the detection of different malicious programs based on their respective binary codes. Malware specifications differ from "standard" software specifications in crucial aspects. Most importantly, a software specification is usually written in the context of the program to be analyzed, i.e., the specification is created with the assistance of the programmer.

Most malware families have similar behaviour and properties, which the majority of scanners use as signatures to detect malware variants. For instance, one of the properties of a worm is self-replication a worm tries to spread by simply copying itself to a host machine through the communication channels of other infected machines. On the other hand, a virus will attempt to spread by a carrier such as an infected file or a media drive. In the following we will examine some common environments and the behaviour of malware.

In the feature selection method the features are either picked manually from the data monitored or by using a specific feature selection tool. The most suitable features are selected by handpicking from the feature spectrum based on the prior knowledge about the environment that the malware are monitoring. For example features that can distinguish certain type of

traffic from the traffic flows are picked for the network traffic model training. The idea behind the feature selection tools is to reduce the amount of features into a feasible subset of features that do not correlate with each other.

In order for malware to perform its malicious functionality and to infect other victims, some components or resources should exist. Malware writers usually develop their code for a particular operating system. For instance, Win32 viruses are effective against Microsoft Windows and may not work on other operating systems. Moreover, a malware may require that some particular applications are running on the victim system in order to be effective.

Malware uses common methods of transmission between computer systems. One of the traditional methods, and the easiest, of transmit-ting malicious programs is via external media such as USB devices and memory disks; however, the rate of spreading malware using this method is considered low compared to other methods such as through networked systems. Malware writers find networked computer systems an excellent environment to replicate and spread their viruses and worms; therefore, inadequate security on a network means that a large number of systems are vulnerable to malicious attacks. Another means of malware infection between computer systems is electronic mail (e-mail). Malicious code can spread easily as a file attachment sent with an e-mail message to as many as possible e-mail users.

The rest of this paper is organized as follows in the first section we describe an introduction of about the content based image classification introduction. In section II we discuss about the Malware detection techniques. In section III we discuss about the proposed method and architecture model for Malware detection classification. In section IV we discuss about the experimental result analysis and comparative study for both techniques, finally in section V we conclude the about our paper which is based on the literature survey and specify the future scope.

II MALWARE DETECTION TECHNIQUES

Techniques used for detecting malware can be categorized broadly into two categories: anomaly-based detection and signature-based detection. An anomaly-based detection technique uses its knowledge of what constitutes normal behavior to decide the maliciousness of a program under inspection. A special type of anomaly-based detection is referred to as specification based detection. Specification based techniques leverage some specification or rule set of what is valid behavior in order to decide the maliciousness of a program under inspection. Programs violating the specification are considered anomalous and usually, malicious. Signature-based detection uses its characterization of what is known to be malicious to decide the maliciousness of a pro-gram under inspection. As one may imagine this characterization or signature of the malicious behavior is the key to a signature-based detection method's effectiveness.

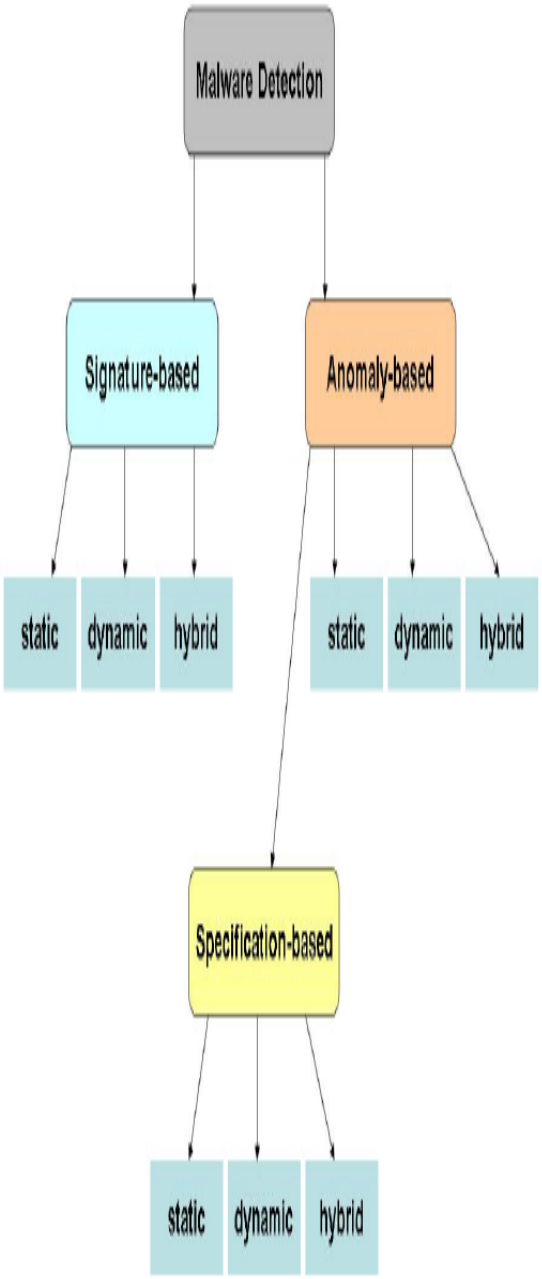

Figure 1: **A classification of malware detection techniques.**

III PROPOSED WORK

In this paper we proposed a malware detection technique based on feature selection in neural network classifier and support vector machine. Feature selection is important part of malware detection or classification technique. The property of malware data is very diverse and unformatted. For the formatting of malware data used preprocessing technique of data mining. Here we used the malware detection with support vector machine and found better results than the other neural network classification techniques.

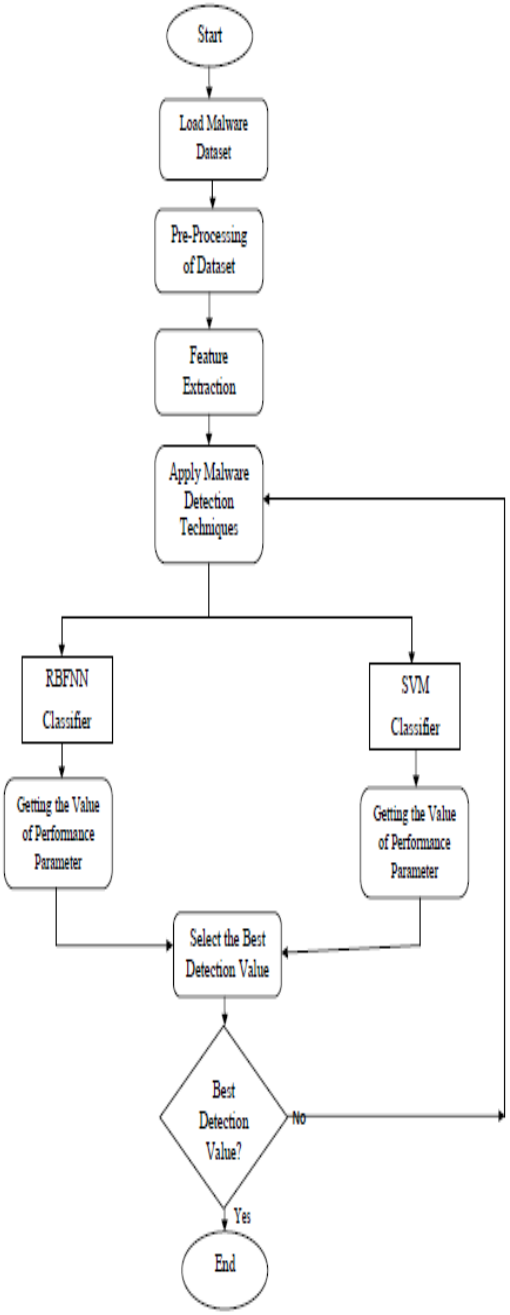

Figure 2: **Proposed model for Malware detection.**

IV EXPERIMENTAL RESULT ANALYSIS

To evaluate the performance of proposed method of content based image retrieval or classification we have use MATLAB software with a variety of image dataset used for experimental task. Here we compare that our empirical result evaluation using the both techniques on which one is based on unsupervised learning and another one is based on supervised learning.

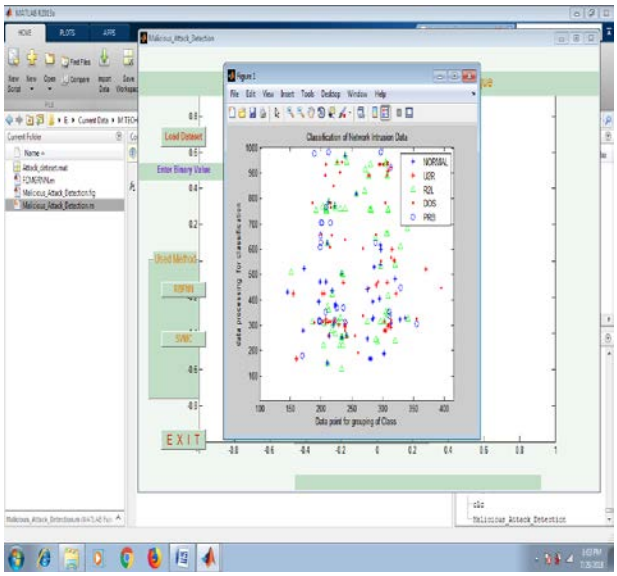

Figure 3: **Shows that the intrusion data classification, when the number of generating value is 0.1 and the method is Radial basis Function Neural network.**

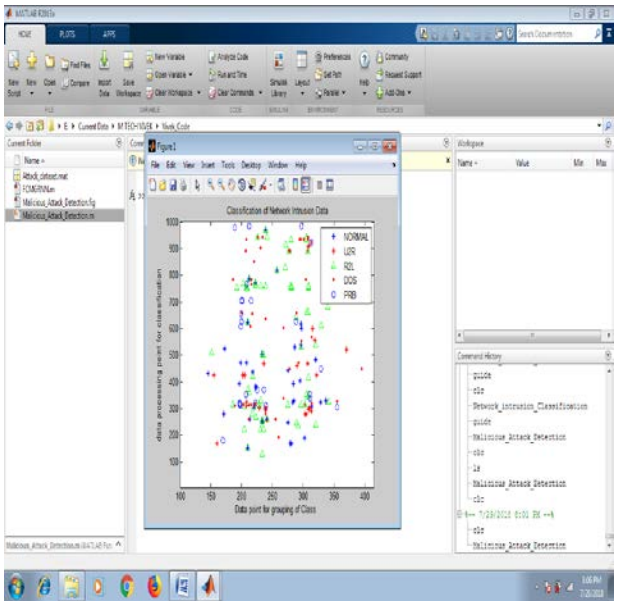

Figure 4: **Shows that the intrusion data classification, when the number of generating value is 0.1 and the method is Support vector machine classifier.**

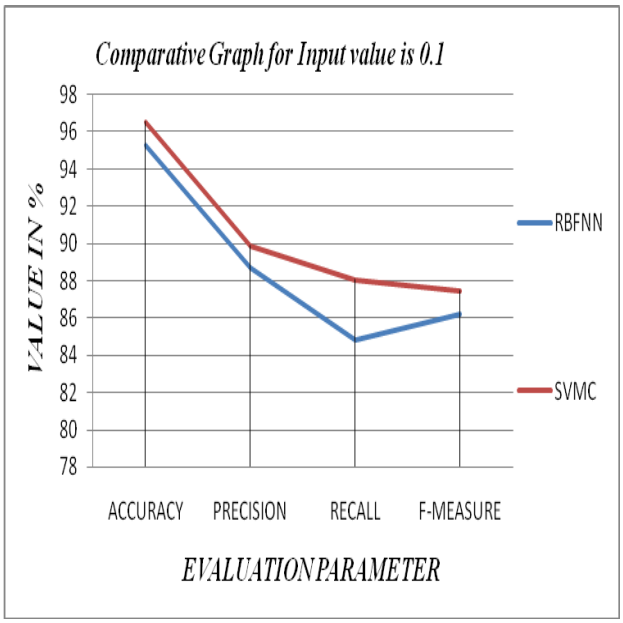

Figure 5: **Shows that the comparative result graph for the Radial basis function neural network and Support vector machine classifier gives the Classification Accuracy, Precision, Recall and F-Measure performance parameters for the given number of input value i.e. 0.1**.

V CONCLUSIONS AND FUTURE WORK

Malware categorization is major challenge in the field of malware detection and writing a program of antivirus. The malware software are self-propagated program infect the system and application software. Now a days for the detection of malware various technique are used such as data mining, neural network and some statically tool. Effectiveness of the malware detection system depends on the ability to early detection of the presence of a malware. In this paper we present the comparative performance evaluation for the Malware detection using neural network and support vector machine, in future we focus increase the detection ratio using some optimization method and also resuce the computation time.

REFERENCES:-

[1] Vittorio P. Illiano, Luis Mu~noz-Gonz_alez, Emil C. Lupu, "Don't fool Me!: Detection, Characterisation and Diagnosis of Spoofed and Masked Events in Wireless Sensor Networks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 14, NO. 3, MAY/JUNE 2017. Pp 279-293.

[2] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, Mani Srivastava, "PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks", COMPUTER-COMMUNICATIONNETWORKS, 2015. Pp 1-12.

[3] Vittorio P.Illiano, Rodrigo V. Steiner, Emil C. Lupu, "Unity is strength! Combining Attestation and Measurements Inspection to handle Malicious Data Injections in WSNs", wisec, 2017. Pp 134-145.

[4] Carlos Lopez, Arman Sargolzaei, Hugo Santana, Carlos Huerta, "Smart Grid Cyber Security: An Overview of Threats and Countermeasures", Journal of Energy and Power Engineering, 2016. Pp 1-13.

[5] Khalid Nasr, Anas Abou El Kalam, Christian Fraboul, "generating representative attack test cases for evaluating and testing wireless intrusion detection systems", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, May 2012, Pp 1-20.

[6] V. Jyothsna, V. V. Rama Prasad, K. Munivara Prasad, "A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, 2011. Pp 26-35.

[7] Nicoleta STANCIU, " Technologies, Methodologies and Challenges in Network Intrusion Detection and Prevention Systems", Informatica Economica, 2013. Pp 144-152.

[8] Howard Chivers, John A. Clark, Philip Nobles, Siraj A. Shaikh, Hao Chen, "Knowing Who to Watch: Identifying attackers whose actions are hidden within false alarms and background noise", 2010. Pp 1-16.

[9] S.V. Annlin Jeba, B. Paramasivan, "False Data Injection Attack and its Countermeasures in Wireless Sensor Networks", European Journal of Scientific Research, 2012. Pp 248-257.

[10] Sunil Gupta, Harsh K Verma, A L Sangal, "Security Attacks & Prerequisite for Wireless Sensor Networks", International Journal of Engineering and Advanced Technology, 2013. Pp 558-567.

[11] T.Kavitha, D.Sridharan, "Security Vulnerabilities In Wireless Sensor Networks: A Survey", Security Vulnerabilities In Wireless Sensor Networks: A Survey, 2010. Pp 31-45.

[12] S.V.Annlin Jeba, B. Paramasivan, "an evaluation of en-route filtering schemes on wireless sensor networks", international journal of computer engineering & technology, 2012. Pp 62-73.

[13] Deepali Virmani, Ankita Soni, Shringarica Chandel, Manas Hemrajani, " Routing Attacks in Wireless Sensor Networks: A Survey", 2015. Pp 1-8.

[14] YOUSEF EL MOURABIT, ANOUAR BOUIRDEN, AHMED TOUMANARI, NADYA EL MOUSSAID, " Intrusion Detection Techniques in Wireless Sensor Network using Data Mining Algorithms: Comparative Evaluation Based on Attacks Detection", International Journal of Advanced Computer Science and Applications, 2015. Pp 164-170.

Vivek Kirar received his Bachelor`s degree in Electronics & Comunication Engineering, in 2013. Currently he is pursuing Master of Technology Degree in Electronics & comunication (Digital communication) from PCST, (RGPV), Bhopal, Madhya Pradesh India. His research area include Wireless sesnor networks.

Mr. **Jitendra Kumar Mishra** he is Associate Professor and Head of the Department of Electronics and Communication Engineering in PCST, Bhopal (RGPV). His received Master of Technology and Bachelor's of engineering respectively in Digital communication from BUIT, Bhopal and from RGPV, Bhopal. He has more than 10 years of teaching experience and publish 25+ papers in International journals, conferences etc. His areas of Interests are Antenna & Wave Propagation, Digital Signal Processing, Wireless Communication, Image Processing etc.