INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Survey on Self Evolving Antivirus Based on Neuro-Fuzzy Inference System

[1]Prof. Sumedh Pundkar, [2]Pratik R. Upadhye

[1]Head Of Department of Computer Engineering
Usha MittalInstitute of Technology,SNDT University
sumedhpundkar@gmail.com
[2]Mukesh Patel School of Technology Management and Engineering, N.M.I.M.S.
JVPD Scheme, Vile Parle,Mumbai, India
Pratik.upadhya@gmail.com

Abstract*: Over the years and as the result of technological developments, the importance of personal computers in our lives has grown significantly. This has resulted in a desire by some to develop malicious applications, whether lone teenagers or nation states, and distribute them across the Internet where they attack a range of computer systems. As a result, the importance of antivirus software has grown significantly and has resulted in an inexorable demand for a dependable antivirus system that can defend against this plethora of malicious viruses. Anti-virus programs are meant to discern computer viruses and protect computers from their actions. In order to guarantee effectiveness and a robust system, antivirus software must be continuously updated and is a perpetual process. This is no small undertaking when taken into consideration the fact that computers connected to the Internet are exposed to viruses from every direction and are delivered using any range of methods: Infected servers and files, USB drives, and more. With today's world filled with information and data, it is very important for us to differentiate which information or data is benign and which is malignant. That is exactly what we aim to develop and implement in the form of our research Adaptive anti-virus using ANFIS architecture. An adaptive anti-virus system that will catch up to the speed at which the viruses update and evolve.*

Keywords: *<Adaptive, Antivirus, Neuro-Fuzzy, ANFIS, virus >*

1. INTRODUCTION

Adaptive antivirus based on Neuro-Fuzzy inference system can be a life time solution to the detrimental viruses and malware actions harming the health and the balance of the system. The primary limitation existing in all prevailing antivirus software security system is its lack of ability to detect new virus definitions at real time and more over it also requires human assistance and update-versions to make the Antivirus system able to detect and repair or block the newly discover viruses or malware. Thus we aim to develop and implement an Antivirus Security System that overcomes such limitations. This Antivirus security system will be self-adaptive and evolving software system that detects unusual behavior and registers this behaviour definition to get accustomed to it for future instances. It will neither need assistance from the developing team nor update-versions which would arrive when damage to the system may have already occurred.

2. LITERATURE REVIEW

The Literature review provides an overview of the various types of anti-virus techniques as mentioned in [1-2].

First-Generation Scanners

Scanners of first-generation [3] typically looked for certain patterns or sequences of bytes called string signatures. Once a virus is detected, it can be analyzed precisely and a unique sequence of bytes extracted from the virus code. This string often called signature of the virus and is stored in the anti-virus scanner database. It must be selected such that not likely is appeared in benign programs or other viruses, optimistically. This technique uses this signature to detect the previously analyzed virus. It searches the files to find signatures of the viruses. It is one of the most basic and simplest methods employed by antivirus scanners.

The anti-virus engine scans the binary code of files to find these strings; if it encounters with a known pattern, it alerts detection of the matching virus.

Second-Generation Scanners

The second-generation scanners [3] introduced exact and almost exact recognition that caused the antivirus scanners became more trustable.

2.1 Generic Detection

"Generic detection" is a term applied when the scanner looks for a number of known variants, using a search string that can detect all of the variants [4]. While it may detect a currently unknown variant in which the same search string can be found, it's only a heuristic detection if it involves the use of a scoring mechanism. Some

Volume 3, Issue III, March 2015
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

systems use a hybrid approach, where a scoring system is added to the generic detection capabilities to give a probability of the variance or family membership with differing degrees of certainty.

2.2 Virus-specific Detection

Sometimes the general virus detection algorithm may not be able to deal with a particular virus [5]. In such conditions, a virus specific detection algorithm must be developed to carry out detection procedure. Actually, this kind of detection is not a regular method, but it denotes any special method that is specifically designed for a given particular virus. This approach is also called algorithmic scanning, but because it can be misleading, we use virus-specific detection term instead of algorithmic scanning.

2.3 Code Emulation

This is one of the strongest detection techniques. It simulates the computer central processor, main memory, storage resources and some necessary functions of operating system by a virtual machine to run the malware virtually and investigate its behavior and performance. The malicious code does not execute on actual machine and it is controlled by the virtual machine precisely, therefore there is no risk for unintentionally propagation of malware. The emulator imitates instructions of the machine by simulating CPU registers and flags, virtually. It resembles the execution of programs and detection procedure analyzes all instructions, individually.

3. ANFIS

Adaptive Neuro fuzzy inference system (ANFIS) is a kind of neural network that is based on Takagi–Sugeno fuzzy inference system [6]. Since it integrates both neural networks and fuzzy logic principles, it has potential to capture the benefits of both in a single framework. Its inference system corresponds to a set of fuzzy IF–THEN rules that have learning capability to approximate nonlinear functions. Hence, ANFIS is considered to be a universal estimator.

Using a given input/output data set, the toolbox function ANFIS constructs a fuzzy inference system (FIS) whose membership function parameters are tuned (adjusted) using either a back propagation algorithm alone, or in combination with a least squares type of method.

This allows your fuzzy systems to learn from the data they are modelling from .A hybrid intelligent system is one that combines at least two intelligent technologies. The combination of probabilistic reasoning, fuzzy logic, neural networks and evolutionary computation forms the core of soft computing, an emerging approach to building hybrid intelligent systems capable of reasoning and learning in an uncertain and imprecise environment.

4. NEW PROPOSED SCHEME

Adaptive antivirus based on Neuro-fuzzy inference system proposes the following functions:-

4.1 USP function or main function:

- Provides antivirus security system software that adapts and evolves itself by detecting unusual behaviour and accustoming itself for future such instances without any human assistance.

4.2 Subsidiary functions:

- Detects or matches the definitions of the code with the existing virus definition present in the software's virus database.
- Alert the user for the same and seeks permission to carry out further action.
- Blocks detected viruses and malware

In this, we provide following parameter as an input parameter

- Severity of virus
- User Knowledge about Virus

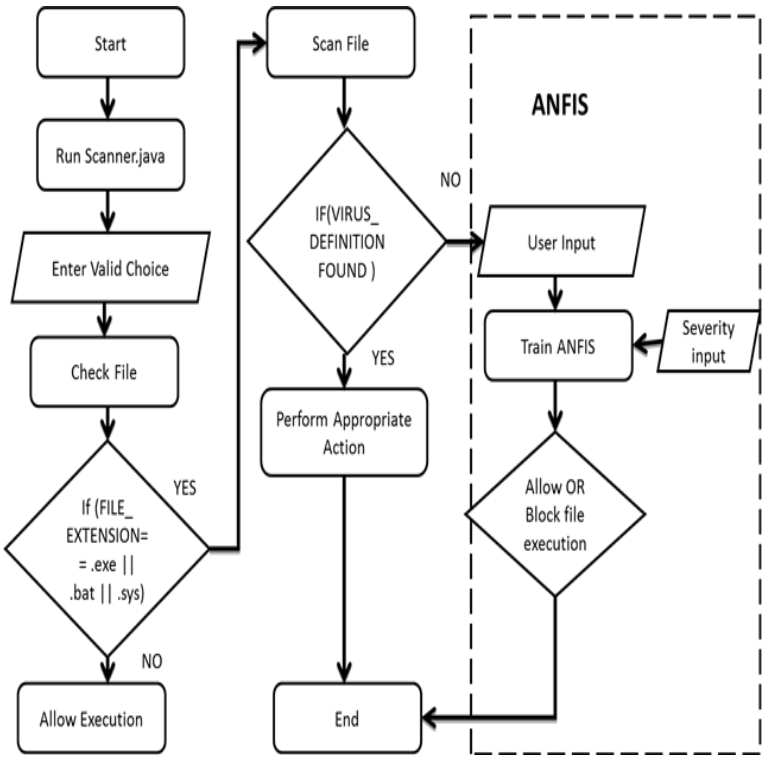

Fig 4.1: Architecture of proposed system

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

5. COMPARISION TABLE

	GEN I	GEN II	GEN III
Need of virus definition	Yes	No	No
Block Level operation	No	Yes	Yes
Analysis of realtime access patterns	No	No	Yes
Memory Resident	No	No	Yes
False Positive	Low	Low	Med-High
False Negative	Low	Low	Medium

The table shows the comparision of the various generations of Antiviruses and the detection of various categories of viruses.

6. Future Work

- Due to the time constraints we are planning to include only 2 parameters as input i.e. User Input and Severity but in future more number of parameters like Type of Viruses, losses and number of occurrences and many other can be added to make it more robust.
- More research has to be done on generating training data which could be feeded to ANFIS for training it.
- Integration MATLAB values into the code
- More Research on Mamdani and Sugeno model and its efficient application in the application.

7. CONCLUSION

- We have started with the implementation of an Antivirus which will take help of Neuro Fuzzy Inference system and generate rules which can help the system to take decisions pertaining to new viruses without human intervention.
- During Literature survey wecame across several systems/applications which were improved and made adaptive using ANFIS approach and evolved into better intelligent systems.
- ANFIS technology could prove to be the best available method for creating Adaptive Antivirus.

REFERENCES

[1] Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011 ISSN (Online): 1694-0814.

[2] Babakbashari Rad, Maslin Masrom and Suhaimi Ibrahim, "Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January, 2011.

[3] Szor, P., The Art of Computer Virus Research and Defense, Addison-Wesley Professional, 2005.

[4] Beauchamp's, P., "Advanced Polymorphic Techniques", International Journal of Computer Science, Vol. 2, No. 3, 2007, pp. 194-205.

[5] Skulason, F., "Virus Encryption Techniques", Virus Bulletin, November 1990, pp. 13-16.

[6] An Adaptive Neural-Fuzzy Approach for Object Detection in Dynamic Backgrounds for Surveillance Systems- IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 59, NO. 8, AUGUST.