International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 3 Issue 6 ǁ June 2015 ǁ PP.06-09

Self Evolving Antivirus Based on Neuro-Fuzzy Inference System

Prof. Sumedh Pundkar[1], Pratik R. Upadhye[2]
[1](Head Of Department of Computer Engineering Usha Mittal Institute of Technology, SNDT University, Mumbai, India)
2(Mukesh Patel School of Technology Management and Engineering, N.M.I.M.S. JVPD Scheme, Vile Parle, Mumbai, India)

ABSTRACT*:* *With today's world filled with information and data, it is very important for one to know which information or data is harmless and which is harmful. Right from cellular phones to big MNCs and Server companies require a security system that is as competent and adaptive as its ever-updating and evolving viruses or malware. The paper talks about the development and implementation of a new idea Adaptive anti-virus based on Anfis logic. An adaptive anti-virus system that will catch up to the speed at which the viruses update and evolve.*

Keywords - *Adaptive, Antivirus, Security, Neuro-Fuzzy, ANFIS, virus*

I. 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 these 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.

II. 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 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.

III. ANFIS

Adaptive Neuro fuzzy inference system (ANFIS) is a kind of neural network that is based on Takagi–Sugeno fuzzy inference system [6]. ANFIS Algorithm was defined by J.-S. Roger Jang in 1992 and since then has played an important role in modeling intelligent self evolving systems. 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

IV. 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 behavior 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

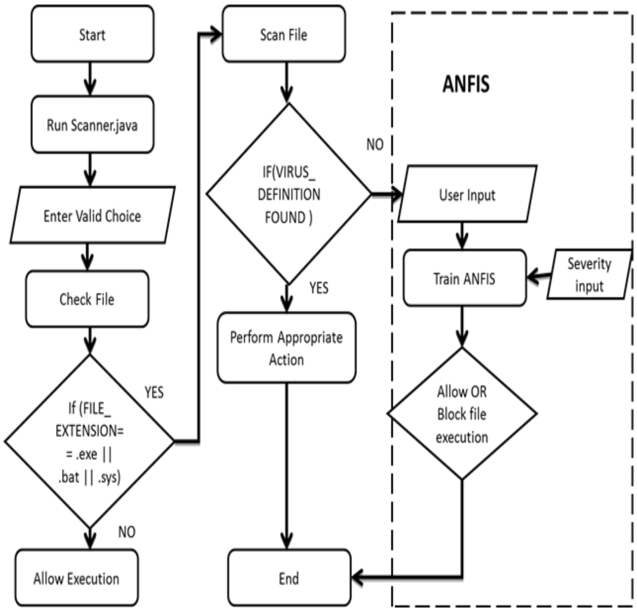

Start
Run Scanner.java
Enter Valid Choice
Check File
If (FILE_ EXTENSION= = .exe || .bat || .sys)
YES
NO
Allow Execution
Scan File
IF(VIRUS_ DEFINITION FOUND)
NO
YES
Perform Appropriate Action
End
ANFIS
User Input
Train ANFIS
Severity input
Allow OR Block file execution

Fig 4.1 Architecture of proposed system

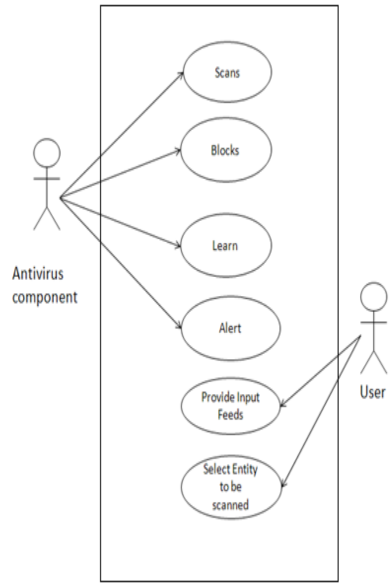
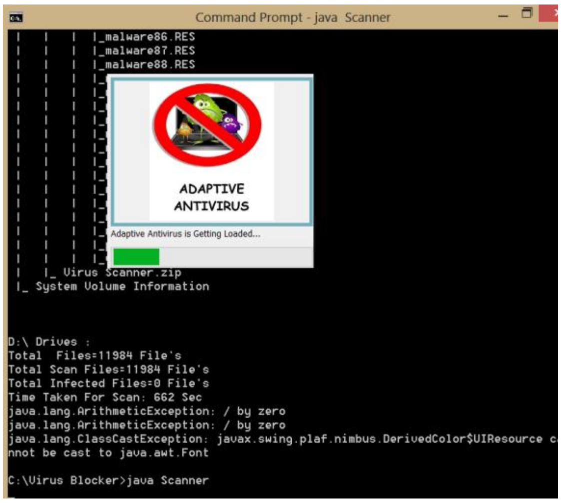


Fig 4.2 Use Case Diagram of the proposed system

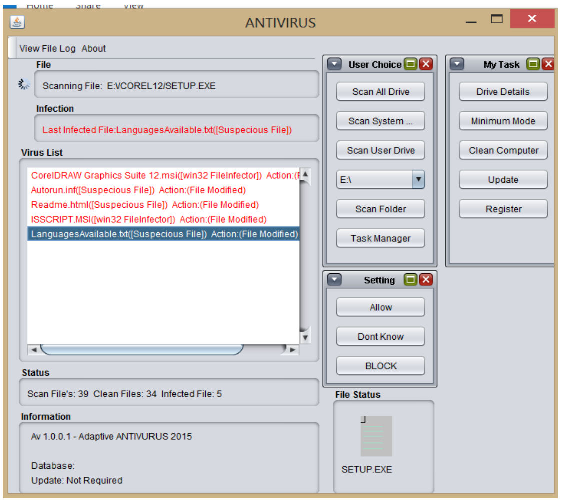
V. WORKING/IMPLEMENTATION OF THE PROJECT


Command Prompt - java Scanner
ADAPTIVE ANTIVIRUS
Adaptive Antivirus is Getting Loaded...

```
 |    |    |   |_malware86.RES
 |    |    |   |_malware87.RES
 |    |    |   |_malware88.RES
 |    |_ Virus Scanner.zip
 |_ System Volume Information


D:\ Drives :
Total  Files=11984 File's
Total Scan Files=11984 File's
Total Infected Files=0 File's
Time Taken For Scan: 662 Sec
java.lang.ArithmeticException: / by zero
java.lang.ArithmeticException: / by zero
java.lang.ClassCastException: javax.swing.plaf.nimbus.DerivedColor$UIResource c
nnot be cast to java.awt.Font

C:\Virus Blocker>java Scanner
```



File

Scanning File: E:VCOREL12/SETUP.EXE

Infection

Last Infected File:LanguagesAvailable.txt([Suspecious File])

Virus List

CorelDRAW Graphics Suite 12.msi([win32 FileInfector]) Action:(F
Autorun.inf([Suspecious File]) Action:(File Modified)
Readme.html([Suspecious File]) Action:(File Modified)
ISSCRIPT.MSI([win32 FileInfector]) Action:(File Modified)
LanguagesAvailable.txt([Suspecious File]) Action:(File Modified)

Status

Scan File's: 39 Clean Files: 34 Infected File: 5

Information

Av 1.0.0.1 - Adaptive ANTIVURUS 2015

Database:
Update: Not Required

File Status

SETUP.EXE

5.1 AV System Start Screen: The Adaptive Anti-Virus based on Anfis starts with this menu where the user selects his arbitrary choice and the Product software performs the selected option.

The Anfis of Adaptive Anti-Virus based on Anfis also referred as Applied Anfis accepts 2 inputs.

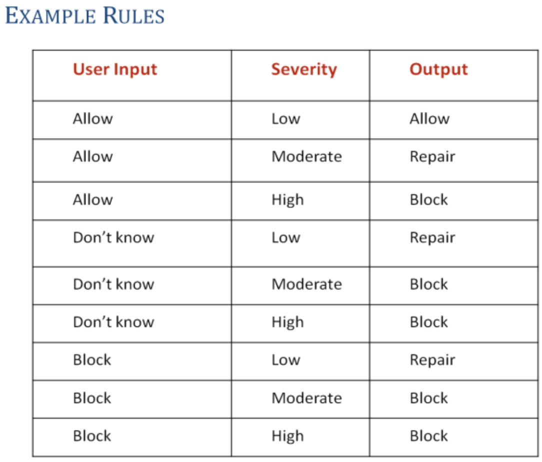
1. User Input(First Input Parameter):

The User Input parameter allows 3 values from the user i.e.

a. Allow   b. Don’t know   c. Block

5.2 Initial design -Functions Overview

- Scans the Entity
- If system matches the signature with existing virus signature ,it is blocked
- If the signature is not matched it then checks/ Detects unusual behavior.
- Block that unusual behavior or action based on User input and Severity
- Adapts and registers the unusual behavior in the database



EXAMPLE RULES

User Input	Severity	Output
Allow	Low	Allow
Allow	Moderate	Repair
Allow	High	Block
Don't know	Low	Repair
Don't know	Moderate	Block
Don't know	High	Block
Block	Low	Repair
Block	Moderate	Block
Block	High	Block

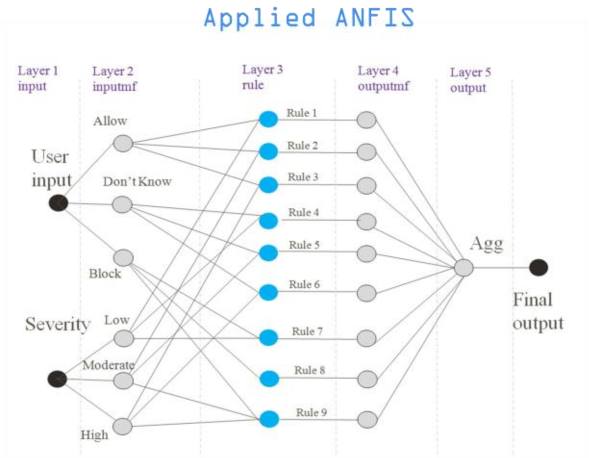


Fig 5.1 Rules and Applied ANFIS for Adaptive Antivirus

VI. CONCLUSION AND FUTURE WORK

ANFIS combines fuzzy logic and neural networks which constitutes a powerful means for designing intelligent systems. Adaptive Antivirus based on ANFIS can be trained using more no. Of parameters into a robust system capable to detect all zero day viruses. Once trained it eliminates the requirement of any kind of expert human intervention for the Anti Virus to Adapt/Update. I have created an experimental dummy system to test the feasibility of the approach . The proposed technique can reduce false positives and false negatives if trained by a Domain Expert and reduce the human intervention and updates required henceforth . Due to the time constraints i have included 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 etc can be added to make it more robust. More Research to be done on Real-time behavioral monitoring of all processes running on a computer, Exhaustive automated and human classification of behaviors and Removal or blocking, depending on threat behavior and likely system impact

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