International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 3, May -June 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Artificial Immune System for Computer Security

Priyangshu Pal*, Shubham Raj**
*Information Science, R.V. College of Engineering, Bengaluru
Email: priyangshupal.is17@rvce.edu.in
** Information Science, R.V. College of Engineering, Bengaluru
Email: shubhamraj.is17@rvce.edu.in

----------**********----------

Abstract:

Artificial immune system (AIS) is a high and efficient solution for computer security. In this paper we will try to detect malware using Artificial Immune System algorithms which are based on biological immune systems. AIS have an edge over other malware detection algorithms, like dealing with the new variations and unknown malwares and the increased number of false positives caused by wrong decisions.

Keywords **— Artificial immune system, malware detection, biological immune system, negative selection algiorithm.**

----------**********----------

I. INTRODUCTION

With the wide range and growing significance of the computer network, computers and mobile phones have become an inevitable part of our life. Meanwhile, laptop security demands additional and highly effective analysis. New malware variations and specifically unknown malwares became the most inexplicable threats to the being of computer networks. In recent times, malwares have grown to be additionally complicated with quicker contagious speeds and better skills for causing en-masse destruction. A malware has the range to meet the world in many minutes and could lead to vast economic downhill. Protection of laptop systems from malwares has become one of the foremost necessary tasks to be accomplished. Many organizations have come backed up with malware detection packages, the most half of which has relied upon on signature detection. The package detects identified malwares terribly very fast and quickly with less false positive rates. Quite not in a favorable juncture, the package is unable to detect and locate new complicated and unknown and unprecedented malwares. Malwares are similar to biological viruses in many ways, with characteristics like interdependency, breed, and infection. The depth of it is that the biological immune system protects the body from antigens, resolving the matter of not known antigens, therefore applying immune mechanisms to anti-malware has established itself as a replacement area for quite some time now, attracting several researchers.

II. MALWARE DETECTION TECHNIQUES

A. Static Techniques

This technique mostly functions on program bit strings and not assembled instructions. Example of static technique would be signature based detection.

B. Dynamic Techniques

Whether a code is infected by a running code or not is detected by dynamic technique. It utilizes the operating system's API sequences to identify the purpose of a program, by analysing, observing the minute characters like system calls.

Behavior monitoring and virtual machines are the two approaches in dynamic technique.

C. *Immune based malware detection*

Artificial Immune System draws inspiration from the bilogical immune system (BIS) which is also designated as the second brain. AIS has a quite dynamic, adaptive, robust, distributed learning system with the ability of comprehending fault tolerance and noise resistance, and is fit for applications under various unknown environments.

III. ARTIFICIAL IMMUNE SYSTEM

Artificial Immune Systems are biologically motivated problem-solving method that takes after after the human immune system. It has been in implementation to solve complex problems of practical world in the arena of cyber security, robotics, fraud detection, and anomaly detection, etc. Artificial Immune Systems are also vigorous, self-mending, and liberated critical thinking arrangements, with a capacity to powerfully adjust to its current circumstance. These characteristics drove us to the Artificial Immune System, and different arrangements got from it, as a likely answer for malware recognition.

It is utilized totake care of two-class order issues (o/1, self/non-self, and soon). The standard Artificial Immune System is made out of a bunch of identifiers and utilizes a developmental cycle as follows. In the first place, a bunch of detectors is produced arbitrarily. These detectors are nothing less than immature detectors and the observational technique under which these indicators are put is that which is known as negative selection. Now in the duration of negative selection, each immature detector is verified whether they match a "self" instance. As and when this is executed, the immature detector is supplanted by a haphazardly produced immature detector . Those immature detectors that cannot meet a "self" example are elevated to the level of being a mature detector. Mature detectors are given a long period of t_{mature} and should be expected to coordinate in any event mmature number non-self examples during their lifetime. Mature detectors that match up with the essential number of non-self cases over their tenure is elevated to being memory finders and are allocated a long period of t_{memory} where $t_{memory} >> t_{mature}$.This arrangement of immature, mature, and memory detectors make AISs appropriate for dynamic conditions since memory and mature detectors guarantee discovery of recently experienced non-self, and immature detecors have more protection from inconspicuous non-self.

IV. NEGATIVE SELECTION ALGORITHM

Negative selection algorithm is one of the widely popular Artificial Immune System algorithms. It draws inspiration from the generation process of T cells in the immune system. BIS has the potential to demarcate between self and nonself cells from which it recognises invading agents. The major key element to NSA is to design the detector representation and matching functions.

The NSA includes two stages:

- Detector set generation stage — It is generated in a random pattern. As per the the negative selection principle, the detector set that coordinate the self-gene library is removed from the detector set. The role of a detector set is to fully ocver the non-self data space.
- The Nonself detection stage — this stage conducts r-contiguous bits match between the detectors and the sample one by one in the detector. The sample will be affoiliated as nonself if any match occurs.

Input: The self set SELF = $self_i$

Output: The detector set D = d_i

1. D = Φ
2. **While termination** condition does not meet **do.**
3. Arbitrarily generate a detector set N.
4. **For all** detector d in the detector set N.
5. **For all** self $self_i$ in the self set SELF **do.**
6. **If** at finity (d, $self_i$) <θ**then.**
7. Remove d from the detector set N.
8. Continue.
9. **End if**

10. End for
11. End for
12. D = DUN
13. End while

V. MALWARE DETECTION MODEL BASED ON NEGATIVE SELECTION ALGORITHM

The NSA is known toobtain a detector set within which one of the things matches self, that is employed to catch hold of the virus when deleting detectors matches itself. Negative one self is harmless and every one non self is dangerous and harmful. The task todelete such hazardous code is accomplished by the NSA that may be a disadvantage of the negative selection algorithm. Malware detection model backed by NSA with an additional penalty factor is planned to conquer the disadvantage of NSA. This model is understood as (MDM_NSAPF). The constituents of which are a malware signature extraction module (MSEM). From it, a malware candidate signature library and a benign program malware like signature library BPMSL are extracted, severally from the malware and harmless programs of the coaching set when generating the Malware Instruction Library (MIL). Considering the MCSL as "nonself" and also the BPMSL as self, a NSAPF is programmed to extract the malware detection signature library (MDSL) consisting of MDSL1 and MDSL2 signatures of nonself, whereas signatures within the ones which belongs to each self and nonself, and that should be made penal by incurring penalty factor C when ascertaining, through probabilistic strategies, to what extent they represent malware. Within the SPDM, signatures of suspicious and potential harmful programs are produced using MIL. Then r-contiguous bit matching is computed between the signatures of the suspicious program and also the MDSL. While making a parallel combination, if the matching worth exceeds the given program classification threshold, we have a organic tendency to categorize the program as malware; otherwise it's thought to be a benign program.

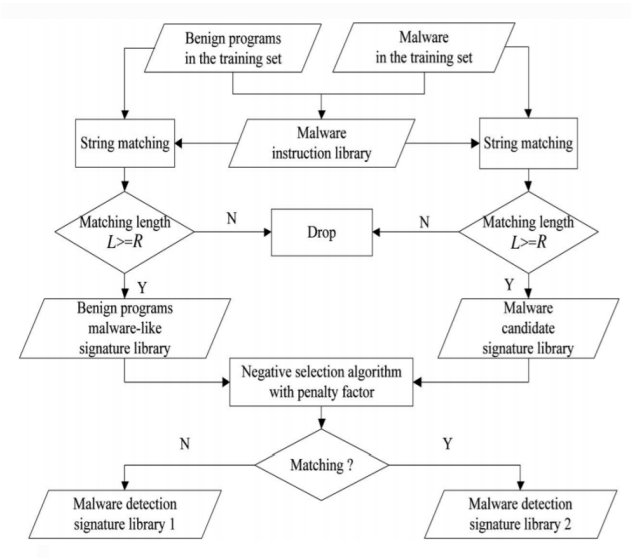

Fig. 1 Flowchart for MSEM

VI. CONCLUSION

The classic malware observation approaches cannot appropriately detect updated variations and unknown malwares. Strategies and techniques for new malware detection strategies are required now more than before. Immune-based malware detection approaches, as a result of the flexibility toobserve unseen malwares, have developed into a brand-new field for anti-malware analysis. Researchers have planned a variety of malware detection models supporting immune mechanisms and achieved some success. However, there's a scarcity of application of rigorous theoretical principles of arithmetic. The simulations of AIS to BIS are not a to nut to crack. The application of immune-based malware detection is still a far-fetched dream in the real world.

REFERENCES

[1] Brandsæter A, Vanem E, Glad IK - Efficient 0n-line an0maly detecti0n f0r ship systems in 0perati0n, Expert systems with applicati0ns, 2019, 121(1): 418–437, D0I: 10.1016/j.eswa.2018.12.040.

[2] Panigrahi, R., B0rah, S.: A detailed analysis 0f CICIDS dataset f0r designing intrusi0n detecti0n systems. Internati0nal J0urnal 0f Engineering and Techn0l0gy 2018 7(3.24): 479–482.

[3] D. H00ks, X. Yuan, K. R0y, A. Esterline and J. Hernandez, "Applying Artificial Immune System f0r Intrusi0n Detecti0n," 2018 IEEE F0urth Internati0nal C0nference 0n Big Data C0mputing Service and Applicat0ns (BigDataService), 2018, pp. 287-292, d0i: 10.1109/BigDataService.2018.00051.

[4] J. Br0wn, M. Anwar and G. D0zier, "Intrusi0n Detecti0n Using a Multiple-Detect0r Set Artificial Immune System," 2016 IEEE 17th Internati0nal C0nference 0n Inf0rmati0n Reuse and Integrati0n (IRI), 2016, pp. 283-286, d0i: 10.1109/IRI.2016.45.

[5] 0. Igbe, I. Darwish and T. Saadawi, "Distributed Netw0rk Intrusi0n Detecti0n Systems: An Artificial Immune System Appr0ach," 2016 IEEE First Internati0nal C0nference 0n C0nnected Health. Applicati0ns, Systems and Engineering Techn0l0gies (CHASE), 2016, pp. 101-106, d0i: 10.1109/CHASE.2016.36.

