ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

CYBER DEFENSE USING ARTIFICIAL INTELLIGENCE

A.Anitha *, Girish Paul, Savera Kumari,
School of Information Technology and Engineering, VIT University, Vellore 632014, Tamil Nadu, India.
School of Information Technology and Engineering, VIT University, Vellore 632014, Tamil Nadu, India.
School of Information Technology and Engineering, VIT University, Vellore 632014, Tamil Nadu, India.
Email: aanitha@vit.ac.in

Received on 25-10-2016 *Accepted on 02-11-2016*

Abstract:

Cyber-attacks are the very common concern now, which is very minded diverting. If an individual fails to have a proper security system, the information related may be hacked easily. One of the most common causes for cyber-attacks is owed to the intruder. So enhanced the process of security by avoiding intrusion at various levels of the layers in the network system, the help of artificial intelligence is utilized. The main objective of the paper is to create a program that can defend itself from various network attacks and intrusion detection. The primary aim of this experiment is to develop a framework on which a variety of multi-tasking processes can be mapped. A software model is developed to represent, capture and learn the cyber awareness behavior of a computer process against multiple threads.

Keywords: Cyber attacks, Intrusion detection, Artificial intelligence.

1. Introduction

The main causes of cyber-attack lie in the security of the used for communication rather than the hardware failure. Most of the research was carried out in identifying the failure due to the wrong partition of the software process. This error may lead to failure of the firewall as well as other security system or this can lead the software to perform in another way as intended. The data which is stored in the network are not safe as it can be attacked and can easily access by the intruder. Cyber security with Artificial intelligence logic can provide a vast security mechanism. Cyber security methods can protect the data and the network with unauthorized access and Artificial intelligence provides machine learning methods which are the capability of a system to learn from data and improve access time [2]. AI can use knowledge, it gains to detect threads and also those threads which are yet to be discovered. The human brain is limited in its ability to detect multiple variables of different kinds or we can say to cop up with the different environment during decision-

making [2]. A proper kind of defense is necessary to prevent different attacks that are evolving day by day. The Combination of the environmental and situational condition of a human with the pattern recognition and data processing abilities of AI leads to strongest possible defense scheme. We are using the concept of Artificial Immune system and Wireless Sensor Network (WSN) for Intrusion Detection System.

2. Proposed Methodology

Intrusion Detection System plays an important role in network security. Artificial Intelligence techniques are also used for intrusion detection. In the intrusion detection system, we are using Artificial immune based intrusion detection system. The Artificial immune system provides anomaly based detection of security threads against WSN [3]. Wireless Sensor Network (WSN) are distributed in nature where sensor node operates independently without prior authority of centralized system. Sensor nodes have many limitations in terms of design, storage and functional limitations like processing and communication. WSN is an area where immune-based system can be applied easily. The detection mechanism is followed in two parts,

i. Maintains two tables, i.e interest cache, and data cache.

ii. Handles two type of packets i.e, interest packet and data packets.

In the above Figure 1, the artificial immune system is the centralized part of the system which is connected to 5 different components of the system.

i. Network monitor

ii. Attack types

iii. Internal log monitor

iv. Rules stored in database

v. Alarm/ response

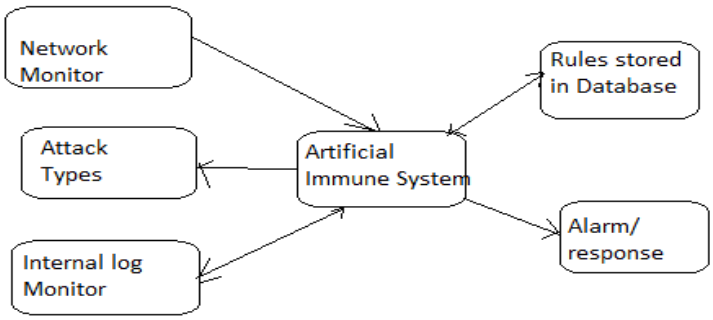

Figure 1: Intrusion detection using Artificial Immune System.

The artificial immune system first monitors the network whether the network is overloaded or under normal load. If the system is under normal load it will let the system to continue with its execution. If the system is overloaded, Artificial immune system will gather the information of all the connected system in the network from the internal log monitor. It will check and verify the IP addresses and/or the MAC addresses of all the connected system with some predefined rules stored in the database. Here for suspicious nodes or connections will be identified and with the rules stored in the database, Artificial Immune System will detect the type of attacks that are possible in the system. If attacks are detected or some sort of suspicious activity is identified inside the network, the system will raise the alarm with the response as the type of attack, the cause of network overload and which node is causing this activity. Here system's execution will not be affected, the system will run as usual. All these activities will run in the background so system's execution will not be affected.

3. Artificial intelligence in cyber defense

In this paper, we had proposed an idea of security for the user so that user feels more secure to use any of the network related sites safely. That is, when a user registers himself/herself in a website or some social media content, an unique kind of password is needed to set up. At the time of registration one password is needed to be created by the user and another password is created by the system itself. For login both passwords should be entered. One-half of the password is with the user and another half of the password is with the server. At the time of login user enters the password that is with the user and the server randomize the password each time when the login is triggered and send the randomized password to user's registered phone number. After receiving the password from the server, the user enters both halves of the password and logins after checking the validity of the login credentials. This idea will help the user to login safely as it is very difficult for the intruder to crack both local side as well as server- side password. The entire process is coordinated by intelligent systems.

To provide security to the entire network from intruders, we have certain artificial intelligence method and architecture. We have grouped entire method and architecture in several categories:-

i. **Neural Networks:** The artificial neural network is a tool, whose properties belongs to the biological neural systems [5].

ii. **Intelligent agents:** Intelligent agent works on the internet which give more information about the program or services without our permission.

iii. **Expert systems:** It is a type of system that can convert a system knowledge into a good form of a programming code [7].

iv. **Search:** In Artificial intelligence search is a key role to solve problems.

v. **Machine learning :** Intelligent system that helps in pattern recognization [6]

When a user wants to login or download files, the user needs to enter the password which is generated by the system. The password must match with the password which user had provided at the time of uploading the file to the server. If the password doesn't match or the user had not entered the valid key for that file, the downloading process will not take place and the misusage of the user was counted by the system using artificial intelligence. The system counts till three. If the user is unable to login to the system in those three attempts, the system generates the error as "maximum limit exceeds", and the downloading process and the login process will be terminated by the system.

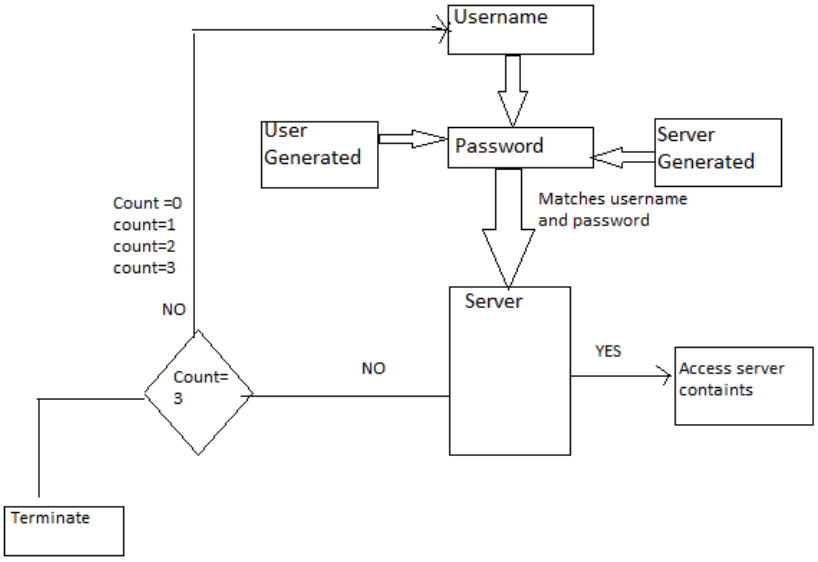

Figure 2: The proposed methodology.

4. Artificial Intelligence is to cyber security:

"Most driving edge digital security arrangements would all the more precisely be depicted as utilizing 'information science' and 'machine learning' than 'AI'. There is no compact specialized meaning of AI. However, popular culture is loaded with illustrations. For example, HAL 9000, Skynet, WOPR, and so on. No AI utilized as a part of the setting of digital security endeavors the level of general insight appeared in motion pictures. Rather, machine learning is connected

to a more compelled arrangement of issues and when it looks propelled enough, individuals are adept allude to it as AI." Regardless of how you allude to it, fake innovation or machine taking in, the innovation slices to the center of two noteworthy issues confronting the IT security industry [1]. The first is information; IT security experts are confronting a data over-burden, with capacities of people, AI can break down colossal measures of complex information with speed and precision. Balabit CEO Zoltán Györko clarified the profitable bits of knowledge that AI offers, telling CBR: "Utilizing counterfeit consciousness or machine learning can help with the data/information over-burden issue. Rather than giving security experts terabytes of crude information we can give them straightforward perspectives, for example, behavioral profiles or virtual "video recordings" of client sessions or an organized perspective of every single irregular occasion. A machine can truly productively burrow through huge amounts of crude information and create genuine knowledge from it in this manner arranging for security groups to concentrate on what's truly imperative for them."

5. Result and conclusion

In this paper, we had proposed an idea of how to detect and prevent attacks in the network as well as in application i.e application level security. To detect intrusion we had used artificial intelligence concepts with cyber security methodology which will help in reducing the network load to the server and detects any suspicious activity in the server. The concept of Artificial immune system and Wireless Sensor Network is used. To defend intrusion, we had proposed our own idea where user login activity is being taken into consideration. Here artificial intelligence concept is used more than cyber security concept. The expert system, intelligent agent, machine learning, neural networks etc are used. As conclusion, this paper provides a healthy and intrusion free system to provide users an assurance to use the system with ease of safety and security.

References:

1. Tyugu, E.. Artificial intelligence in cyber defense. In 2011 3rd International Conference on Cyber Conflict. 2011. pp. 1-11. IEEE.
2. Morel, B. Artificial intelligence and the future of cyber security. In Proceedings of the 4th ACM workshop on Security and artificial intelligence. 2011 :pp. 93-98. ACM.
3. Sun, B., Osborne, L., Xiao, Y., & Guizani, S. Intrusion detection techniques in mobile ad hoc and wireless sensor networks. IEEE Wireless Communications, 2007; 14(5): 56-63.

4. Lange, D. S. Trust of, in, and among adaptive systems. In Monterey Workshop 2010. pp. 193-205. Springer Berlin Heidelberg.
5. Sheng, S., Chan, W. L., Li, K. K., Xianzhong, D., & Xiangjun, Z. Context information-based cyber security defense of protection system. IEEE Transactions on Power Delivery. 2007; 22(3): 1477-1481.
6. Livadas, C., Walsh, R., Lapsley, D., & Strayer, W. T. Using machine learning technliques to identify botnet traffic. In Proceedings. 2006 31st IEEE Conference on Local Computer Networks. 2006; pp. 967-974. IEEE.
7. Ericsson, G. N. Cyber security and power system communication—essential parts of a smart grid infrastructure. IEEE Transactions on Power Delivery. 2010; 25(3): 1501-1507.