International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 24th Mar 2020. Link :http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-03

Title: **AI BEING BENEFICIAL IN DETECTING RANSOMWARE USING IDPS AND MACHINE LEARNING**

Volume 09, Issue 03, Pages: 15-21.

Paper Authors

K. MONICA

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AI BEING BENEFICIAL IN DETECTING RANSOMWARE USING IDPS AND MACHINE LEARNING

K. MONICA
Assistant Professor, Department of computer Science & Engineering, Godavari Institute of Engineering & Technology

Abstract: With the growing usage of technology there are more chances of undergoing information threats. It is equally important to safeguard or information and to use technology. Artificial Intelligence has been playing a prominent role in cyber security with the help of Machine learning being a component of AI. ML applies efforts to constantly improve functions and strategies time to time. Thus by studying and analyzing the behavior of people around it can identify patterns .This paper studies different techniques of Intrusion Detection and prevention techniques using Machine Learning and particularly Ransomware is explained in detailed.

Keywords: AI in cyber security, IDP, Machine learning, Ransomware,

1.Introduction:

Technology has become both a boon and a bane in our daily life. We made our bank accounts get connected to our mobiles and also made our to-do list always available and reminding us the things we need to do in a particular day. What happens if our information gets manipulated what happens if our credentials gets hacked by someone and we need to pay a huge amount to get our information or credentials back? Though we maintain high security to our information the hackers are no less talented to break our securities. Offences that are made against individuals or organizations with a criminal motive to spoil the reputation of organization or individual made the crime to take a different face.There are several examples of cyber crimes such as: unauthorized access to system, theft in online transactions, hacking, DoS,etc.,

Similarly these type of activities are taken as prior importance to combat with making the corporate and government organizations safe.

The few most popular ways of stealing information consists of:

- Phishing
- Skimming
- Malware.

Phishing: Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

Skimming: Skimming is a method used by identity thieves to capture information from a cardholder. Several approaches can be used by fraudsters to procure card information with the most advanced approach involving a small device called a skimmer.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Malware: A Malware attack is a type of cyber attack in which malware or malicious software performs activities on the victim's computer system, usually without his/her knowledge.

2. ARTIFICIAL INTELLIGENCE AND ADVANTAGES

Artificial Intelligence: Artificial intelligence (AI), sometimes called machine intelligence, is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans. Leading AI textbooks define the field as the study of "intelligent agents": any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals. The term "artificial intelligence" is often used to describe machines (or computers) that mimic "cognitive" functions that humans associate with the human mind, such as "learning" and "problem solving".

Advantages of Artificial Intelligence: The advantages of Artificial intelligence applications are enormous and can revolutionize any professional sector. Few of them are listed below:

1. Reduction in Human error
2. Digital Assistance
3. Faster in Decision making

Applications of Artificial Intelligence:

- Robotics
- Education
- Health care
- Cyber Security

3. TYPES OF INTRUSIONS, INTRUSION DETECTION AND PREVENTION SYSTEM

3.1 Intrusion - To compromise a computer system by breaking the security of such a system or causing it to enter into an insecure state. The act of intruding—or gaining unauthorized access to a system—typically leaves traces that can be discovered by intrusion detection systems.

3.2.Types of Intrusion Detection:

There are several ways of detection an instrusion. Few among them are as follows:

- Phishing Detection.
- Network Intrusion Detection.
- Social Network Spam Detection
- Malware Detection.
- Lateral Movement
- Ransomware.

Of the above listed detection we will be learning Ransomware Detection in detail.

3.2.1 Ransomware:

Ransomware is a kind of malignant application from the cryptovirology that jeopardizes to broadcast the prey's details or hinder approach to it unless a payment is made to the perpetuator. Simple ransomware techniques are effortlessly reversible, whereas, there are some advanced malwares such as cryptoviral blackmail under which victim's data is encrypted and is made unobtainable and claims for a payment to decrypt it.

Appropriately executed extortion attack results in an unmanageable issue where reclaiming the data without decryption key is difficult and digital currencies are accustomed for the ransoms, causing tracing and charging the agents difficult.

Ford et al [1] concludes that Machine Learning is a constructive tool that can be utilized in many fields of cyber security. There exist some robust anti-phishing algorithms and network intrusion detection systems. The machine learning classifiers themselves are liable to harmful attacks despite the fact that machine learning helps keeping various systems secure. There are many opportunities in information security to apply machine learning to address various challenges in such complex domain.

According to [2] , the safety of computer systems from high- tech cyber-attacks is one of the major concerns for national and international security. Artificial intelligence and Machine Learning play a noteworthy role in protection of computer systems. Numerous researches have been organized using certain datasets. [2] observes comprehensive class of various datasets together with their advantages and disadvantages.

The researcher [3] remarks that machine learning is a robust tool that can be used for automating complex defense cyber activities and threats. The researcher holds the position for the basis of future research that can focus on scrutinizing existing security solutions and the various challenges influencing machine learning to develop and deploy extensible cybersecurity systems in production environments.

[4] Suggests that exclusive or intimate facts of an individual along with the crucial framework is liable to numerous cybercrimes. Likewise situations, Machine Learning is serving mankind efficiently in focusing on the issues of cyber security considering its intelligent kind and adaptability. Scholarly assets have exhibited that there are several applications of Machine learning which assist the human to defend against rigorous cyber-attacks, furthermore constituting the phenomenon that plenty more is yet to be researched in the pot of opportunities of Machine learning.

The researcher [4] precisely conferred the progress formed in exercising numerous procedures of Artificial intelligence, their present position and the area of subsequent work.

3.3. Intrusion Detection System (IDS)

IDS can offer protection from external users and internal attackers, where traffic doesn't go past the firewall at all. The firewall defend an organization from malicious attacks from the Internet and the IDS if someone tries to break in through the firewall or manages to break in the firewall security then tries to have access on any system in the trusted side. It alerts the system administrator in case there is a breach in security. An IDS is like a smoke detector, that raise an alarm if specific things occur.

An Intrusion Detection System (IDS) is a device or software that monitors

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

network or system activities for malicious activities or policy violations and produces reports to a management station. IDS can be Network-based Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS) [5].

IDS performs a variety of functions [6]:

- Monitoring users and system activity
- Auditing system configuration for vulnerabilities and misconfigurations
- Assessing the integrity of critical system and data files
- Recognizing known attack patterns in system activity
- Identifying abnormal activity through statistical analysis
- Managing audit trials and highlighting user violation of policy or normal activity
- Installing and operating traps to record information about intruders
- Correcting system configuration errors

An **intrusion detection and prevention system (IDPS)** (See Fig. 1) is a software or hardware device placed inside the network, which can detect possible intrusions and also attempt to prevent them [8].

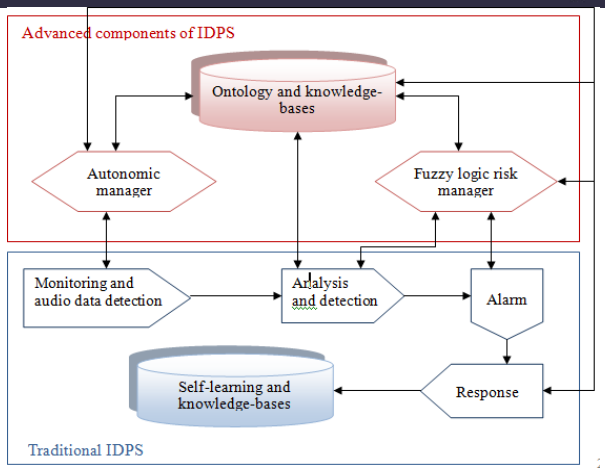

Figure 1: IDPS based on AI

Artificial Neural Networks (ANNs) can enhance the performance of Intrusion Detection Systems (IDS) when compared with traditional methods [17]. Artificial neural networks are a stepping stone in the search for artificial intelligence. ANNs is an information processing system which is inspired by biological nervous system. ANN has tools through which we can develop AI [8].

3.3.1 Desired Characteristics of an IDPS

An IDPS should have certain characteristic in order to be able to provide efficient security against serious attacks. Those characteristics include the following [7]:

- Real-time intrusion detection – while the attack is in progress or immediately afterwards,
- False positive alarms must be minimized,
- Human supervision should be reduced to minimum, and

continuous operation should be ensured,

- Recoverability from system crashes, either accidental or those resulting from attacks,
- Self-monitoring ability in order to detect attackers' attempts to change the system,
- Compliance to the security policies of the system that is being monitored, and
- Adaptability to system changes and user behavior over time.

4.APPLICATIONS OF AI TO DEFENSE AGAINST CYBER CRIMES

Available academic resources show that AI techniques already have numerous applications in combating cyber crimes. For instance, neural networks are being applied to intrusion detection and prevention, but there are also proposals for using neural networks in "Denial of Service (DoS) detection, computer worm detection, spam detection, zombie detection, malware classification and forensic investigations" [9]. AI techniques such as Heuristics, Data Mining, Neural Networks, and AISs, have also been applied to new-generation anti-virus technology [11]. Some IDSs use intelligent agent technology which is sometimes even combined with mobile agent technology. Mobile intelligent agents can travel among collection points to uncover suspicious cyber activity [10]. Wang et al. (2008) stated that the future of anti-virus detection technology is in application of Heuristic Technology which means "the knowledge and skills that use some methods to determine and intelligently analyze codes to detect the unknown virus by some rules while scanning" [11]. This section will briefly present related work and some existing applications of AI techniques to cyber defense.

4.1. Artificial Neural Network Applications

ANN is a computational mechanism that simulates structural and functional aspects of neural networks existing in biological nervous systems. They are ideal for situations that require prediction, classification or control in dynamic and complex computer environments [12].

Chen (2008) designed NeuroNet – a neural network system which collects and processes distributed information, coordinates the activities of core network devices, looks for irregularities, makes alerts and initiates countermeasures. Experiments showed that NeuroNet is

effective against low-rate TCP-targeted distributed DoS attacks [13].

4.2. Intelligent Agent Applications

Intelligent agents are autonomous computer-generated forces that communicate with each other to share data and cooperate with each other in order to plan and implement appropriate responses in case of unexpected events. Their mobility and adaptability in the environments they are deployed in, as well as their collaborative nature, makes intelligent agent technology suitable for combating cyber attacks.

4.3. Artificial Immune System Applications

AISs, just like the biological immune systems which they are based on, are employed to uphold stability in a changing environment. The immune-based intrusion detection comprises the evolution of immunocytes (self-tolerance, clone, variation, etc.) and antigens detection simultaneously. An immune system produces antibodies to resist pathogens and the intrusion intensity can be estimated by variation of the antibody concentration. Therefore, AISs play an important role in the cyber security research [14].

5.HOW CAN ML CHANGE THE STATE OF CYBERSECURITY

Considering the condition of the implementation of ML systems can be a real game changer. Certainly, 52% of cyber professionals presume that current systems are not precise enough. However, these systems are benefited with abilities that will empower cyber security professionals with abundant possibilities to defend against cyber-attacks and secure their company. Today, techniques, like machine learning and deep learning, are probable because of more effective algorithms and the large amounts of available data.

6.CONCLUSION

In this paper, we have seen various attacks threatening the cyber space, and different techniques to deal with the same. Machine learning and Artificial Intelligence techniques have given enterprises the capability to ensure the safety of its data. Furthermore, these techniques are themselves vulnerable to various malignant attacks.

7. REFERENCES:

[1] S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, “A Comparison of Machine Learning Techniques for Phishing Detection”, APWG eCrime Researchers Summit, October 4-5, 2007, Pittsburg, PA USA: IGI

[2] Md. Zeeshan Siddiqui &Sonali Yadav, Application Of Artificial Intelligence In Fighting Against Cyber Crimes: A Review, International Journal of Advanced Research in Computer Science April 2018 , (ISSN: 0976-5697), ISBN: 978-93-5311-643-9, page[118-121]

[3] ManjeetRege& Raymond Blanch K. Mbah, Machine Learning for Cyber Defense and Attack , DATA ANALYTICS 2018 : The Seventh International Conference on Data Analytics, Copyright (c) IARIA, 2018. ISBN: 978-1-61208-681-1 , pp.73–78.

[4] Nilaykumar Kiran Sangani&HarootZarger, Machine Learning in Application Security, [Accessed: March 18, 2019] http://dx.doi.org/10.5772/intechopen.68796

[5]Wikipedia, "Intrusion detection system", en.wikipedia.org, Available:http://en.wikipedia.org/wiki/Intrusion_detectio_system

[6] Gang Wang, Jinxing Hao, Jian Ma, and Lihua Huang, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering", Elsevier Ltd 2010

[7] A. Patel, Q. Qassim, Z. Shukor, J. Nogueira, J. Júnior, C. Wills, (2010) "Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System," Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), Port Elizabeth, South Africa, May 17-18, 2010.

[8] Selma Dilek, Hüseyin Çakır and Mustafa Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review", International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, January 2015

[9] E. Tyugu, (2011) "Artificial intelligence in cyber defense", 3rd International Conference on Cyber Conflict (ICCC 2011), pp. 1–11.

[10] D. Dasgupta, (2006) "Computational Intelligence in Cyber Security", IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS 2006), pp. 2–3

[11] X. B. Wang, G. Y. Yang, Y. C. Li, D. Liu, (2008) "Review on the application of Artificial Intelligence in Antivirus Detection System", IEEE Conference on Cybernetics and Intelligent Systems, pp. 506 509.

[12] C. Bitter, D.A. Elizondo, T. Watson, (2010) "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection", IEEE World Congress on Computational Intelligence (WCCI 2010), pp. 949 – 954.

[13] Y. Chen, (2008) "NeuroNet: Towards an Intelligent Internet Infrastructure", 5th IEEE Consumer Communications and Networking Conference (CCNC 2008), pp. 543 547.

[14] L. Rui, L. Wanbo, (2010) "Intrusion Response Model based on AIS", International Forum on Information Technology and Applications (IFITA), Vol. 1, pp. 86 – 90.