IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

COMBATING CYBER CRIME: EXPLORING THE ROLE OF AI

[1]Mansi Pathak, [2]Shriya Arora
[1]Student, [2]Student
Department of Engineering and Technology
Guru Nanak Dev University, Amritsar, India

Abstract:
By the use of global technological advancements, criminals are using cyberspace to commit numerous cyber-crimes. People are connected to the cyber space with personal a device that's why they are all vulnerable to interferences and a variety of threats. Internet security suits are the basic protection methods and these are not just enough to protect the data and devices. Highly Advanced cyber defense systems have become essential. As of today, with the technology, AI plays a major role in technology and has been involved with many technological aspects as well. By today, creating cyber defense systems, using AI has become a trend. The basic idea of this study is to establish a classy cyber-crime defense system which involves intelligent agents that are based on artificial intelligence.

Keywords: **Cyber-crimes, Intrusion detection and prevention system, artificial agents, artificial intelligence.**

I.INTRODUCTION

This research paper mainly focuses on how to contest cybercrimes, and also it reveals how AI and its effective tool "agent" can be used in detection and prevention of cyber-attacks. On the IT industry, Cyber-attacks tend to have a huge impact when it comes to data theft from many societies across the world or systems which depend on web applications. As web applications are used increasingly, they have become a very vulnerable and a popular target for security attacks. Any action that avoid the security rules of the targeted system using a computer and a network can be defined as a cybercrime. The computer might be used as a burglar or it can be the target in a cybercrime. The content of the paper has been divided into the explanation of the characters or components which are being used in other related research papers. Solution for the identified problem is given in the paper.

II. IDENTIFY, RESEARCH AND ACCUMULATE IDEA

Cyber attacking, it is a widespread statement used in the modern world. On a daily basis, thousands of computer networks or systems get attacked by an unknown hacker in order to smash up or demolish the whole system. In order to secure and identify such security attacks many systems and methods are being developed. In order to identify the available technologies, mechanisms etc, a background study was done.

S.No	Name	Description
1	Intrusion Detection System	An ID system is a network security technology formerly built for spotting susceptibility that exploit against a targeted application or a computer system. It is the procedure of monitoring the incidents occurring in a computer system or in a network and examining for potential risk alerts. Meticulous interrupters can be pointed and shown through an algorithm [2] [9] [10]. Intrusion detection system (IDS) only can identify interrupters, and it cannot secure the system from attacks [5] [7]. It should be fast enough to identify the interrupters (external or internal intruders) as soon as the attack is going on Intrusion Detection System prioritizes efficiency as a key feature. Intrusion Detection System (IDS) technologies are not very effective as there are several limitations, such as performance, scalability and flexibility.
2	Intrusion Prevention System	Intrusion Prevention System (IPS) is a novel approach for safeguarding networking systems. The IPS provides a paired or connected layer of analysis that uses for dangerous content because it often lies behind the firewall. The IP system is a defensive approach to network security that is used to identify potential threats and respond to them quickly. Intrusion prevention systems also have the ability to take immediate actions; it's about a group of rules created by the network administrator [9]. Particularly, the group of rules includes: 1. Dropping the malicious packets. 2. Send an alarm to the administrator. 3. Blocking traffic from the source address. 4. Resetting the connection. The IPS should work as one of the main vanguard components used to avoid the degrading of network performance.
3	Cyber Security System / Cyber Attack Detection Systems (CADS)	Cyber Attack Detection Systems (CADS) and its generic framework are based on the GDA algorithm. This algorithm is employed for feature decrement of the cyber-attack datasets and a collective approach of classifiers for the classification of cyber-attacks [1] [10]. Cyber Attack Detection System is having superior detection correctness for all the classes of attacks. There are two types of Cyber Attack Detection Systems (CADS) [2]. 1. Host Intrusion Detection Systems (HIDS) 2. Network Intrusion Detection Systems (NIDS).
4	Detects denial-of-service (DOS) attacks	A DoS attack is an attack type that is used to make a computer or a network resource engaged to the users, either temporarily or permanently suspending the services of a host connected to a network. If the user is trying to access the internet, an attacker may be able to prevent the user from accessing email, websites, online accounts (banking, etc.), or other products and services that reside on the affected computer. DoS attack is a situation where an intruder floods a network with information and it's the most common type of DoS attack. After that, the user will not be able to access that site. There are many other types of cyber-attacks such as brute force attacks, browser attacks, shellshock attacks, SSL attacks, backdoor attacks, and botnet attacks [3] [6] [7].
5	Agent Based / Artificial Agent	An agent is an entity that can be activated, self-directed, and has the capability of formulating inner decisions can recognize as an agent. An agent is a software program that gives support to the user to achieve some

		duties or activities. Agents in a multi-agent system (MAS) work together with every user of the system [4] [8]. For the purpose of communication, a common language is required, that is Agent Communication Language, or ACL. They may have features such as mobility, adaptability, and collaboration. To learn or exchange experiences, multiple agents interact with each other in a multi-agent system. [4] [8].
6	Algorithms	For solving a problem, an algorithm can be identified as a procedure or a formula. To detect and defeat cyber-attacks, new approaches can be made by combining a set of algorithms [5] [9]. Integrating Fuzzy logic and Genetic algorithms (GA) to pinpoint attackers has been developed since there is an essentiality of a high-security approach to safe and confident communication of information between different organizations [7]. Genetic Algorithm is used to find appropriate fuzzy rules which is a machine learning algorithm. And it gives a more powerful performance.
7	Data sharing between agents	In sharing data, the organization has used a wide variety of sharing methods such as centralized data reporting on one side and decentralized sharing on the other and agents sharing its relevant information with other agents in the system [8].
8	Data mining	Data mining, also known as data or knowledge discovery is the process of scrutinizing data from different perspectives and transforming it into meaningful insights. It allows for investigating data from many different scopes; classifying it, and shortening the identified relationships. Broadly speaking, data mining involves the procedure of discovering links or blueprints among fields in large relational databases. Identifying earlier cyber attacking details using data mining procedure predictions can be done regarding future attacks [10].

III. APPLICATIONS OF AI TO DEFENSE AGAINST CYBER CRIMES

AI techniques already have several applications for fighting against cybercrimes. For example, neural networks are being applied to “Intrusion Detection and Prevention”, but some applications “Denial of Service (DoS) Detection”, “Computer Worm Detection”,” Zombie Detection”, “Malware Classification”, “Spam Detection” and “Forensic Investigations” are also used Neural Network[5]. Artificial intelligence techniques (Heuristics, Data Mining, Neural Networks, and AISs), have been employed to the most recent anti-virus technology [7]. Mobile agent technology uses intelligent agent technology which is sometimes combined with IDSs. Mobile intelligent agents can uncover suspicious cyber activity by moving among collection points [2]. This paper will briefly present related work and several presented applications of AI techniques to cyber defense.

S.No	Name	Description
1	Artificial Neural Network Applications	ANN is a computational method that replicates structural and practical phases of neural networks presented in biological nervous systems. They are ideal for situations that require prediction, categorization, or manage in dynamic and multifaceted computer environments [12] [14].
2	Intelligent Agent Applications	Intelligent agents are independent and self-directed computer generators to 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 [11]. Their collaborative nature, mobility, and adaptability in the environments make intelligent agent technology suitable for combating cyber-attacks.
3	Artificial Immune System Applications	In a changing environment, AISs are employed to uphold stability. The immune-based intrusion detection comprises the evolution of self-tolerance, genetic copy, variation, and antigens recognition simultaneously. An immune system synthesizes antibodies to combat pathogens and the intrusion intensity can be evaluated by fluctuation of

		the antibody concentration. Therefore, In the cyber security research AISs play an important role [13] [15].
4	Genetic Algorithm and Fuzzy Sets Applications	In cybercrime detection and prevention, Numerous bio-inspired computing methods of Artificial Intelligence have been increasingly playing an important role [16]. AI agents applied their algorithm to an artificial computer security system and showed its effectiveness in intrusion detection.
5	Other AI Applications	Intelligent Agents proposed a hybrid approach, focused on improving the performance of intrusion detectors of IDSs which uses the searching performance of an immune algorithm to generate fuzzy detectors [17]. The research showed the great searching ability of the immune algorithm. Fuzzy detection rules reduce the frangibility of detectors and improve the detection precision as results showed.

IV. LIMITATIONS OF CURRENT ANOMALY DETECTION/PREVENTION SYSTEMS

There have some limitations that need to be handled although different detection systems offer the opportunity to identify earlier anonymous attacks. The major problem is the complexity of making an unyielding model of what adequate actions are and what an attack is; therefore, they may give a huge amount of false positive alarms, which may be caused by unusual behavior that is actually normal and certified, since normal behavior may easily and willingly change. Other limitations include the following [11, 12, and 15].

• The results can be very unfortunate since it will attempt to stop the activity or change it if the detection and prevention system inaccurately classifies a justifiable activity as a malicious one.

• If attackers can learn how the system works intrusion detection system, no matter how efficient, may be disabled by attackers.

• In diverse situations there is also an issue of integrating information from different sites.

V. FUTURE WORK

To have better results there are things which can be improved in future. Agents have no ability to identify upcoming attacking strategies although they can help to improve IDSs in many areas. In order to moderate this problem, agents must be planned with the aptitude of forecasting the future of attack types. The area of agent system technology is progressively developing and is being built. To bring the mentioned technologies to the same level, there should be new designs and implementations. In order to overcome the issues mentioned above new methodologies must be introduced.

VI. CONCLUSION

Information technology considerably has a fast impact on human lifestyles. On the other hand, it also produces questions such as the emergence of cybercrimes. In the fight against cyber-crimes, the application of artificial agents is a novel trend as they provide features such as portability rationality, adjustability, and collaboration. This paper has presented the cyber-crimes and advantages of applying artificial agent techniques in relationship with Intrusion Prevention Systems, Intrusion Detection Systems, Cyber Attack Detection Systems, and algorithms in categorize to combat cyber-crimes, as well as given the scope for future work.

VII. REFERENCES

[1] R. Hill, "Dealing with cyber security threats: International cooperation, ITU, and WCIT", 2015 7th International Conference
on Cyber Conflict: Architectures in Cyberspace, pp. 119-134, 2015 [Online]. Available: http://ieeexplore.ieee.org/xpl/abstractReferences.jsp?tp&arnumber=7158473&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D715 8473. [Accessed: 13- Feb- 2016].

[2] S. Singh and S. Silakari, "A Survey of Cyber Attack Detection Systems", IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 5, 2009 [Online]. Available: http://paper.ijcsns.org/07_book/200905/20090501.pdf. [Accessed: 08- Feb- 2016].

[3] J. Nogueira, "Mobile Intelligent Agents to Fight Cyber Intrusions", The International Journal of FORENSIC COMPUTER SCIENCE, vol. 1, pp. 28-32, 2006 [Online]. Available: http://www.ijofcs.org/V01N1-P03%20-%20Mobile%20Intelligent%20Agents.pdf. [Accessed: 10- Feb- 2016].

[4] S. Adebukola, Onashoga, Akinwale O. Bamidele and A. Taofik, "A Simulated Multiagent-Based Architecture for Intrusion Detection System", (IJARAI) International Journal of Advanced Research in Artificial Intelligence, vol. 2, no. 4, 2013 [Online]. Available: http://thesai.org/Downloads/IJARAI/Volume2No4/Paper_6A_Simulated_MultiagentBased_Architecture_for_Intrusion_Detection_System.pdf. [Accessed: 15- Jan2016].

[5] S. Dilek, H. Çakır and M. Aydın,"APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNIQUES TO COMBATING CYBER CRIMES: A REVIEW", International Journal of Artificial Intelligence & Applications (IJAIA), vol. 6, no. 1, 2015 [Online]. Available: http://arxiv.org/ftp/arxiv/papers/1502/1502.03552.pdf. [Accessed: 13- Feb- 2016].

[6] J.Raiyn, "A survey of Cyber Attack Detection Strategies", International Journal of Security and Its Applications, vol. 8, no. 1, pp. 247-256, 2014 [Online]. Available: http://www.sersc.org/journals/IJSIA/vol8_no1_2014/23.pdf. [Accessed: 13- Feb- 2016].

[7] A. Cerli and D. Ramamoorthy, "Intrusion Detection System by Combining Fuzzy Logic with Genetic Algorithm", Global Journal of Pure and Applied Mathematics (GJPAM), vol. 11, no. 1, 2015 [Online]. Available: http://ripublication.com/gjpamspl/gjpamv11n1spl_20.pdf. [Accessed: 09- Feb- 2016].

[8] O. Oriola, A. Adeyemo and A. Robert, "Distributed Intrusion Detection System Using P2P Agent Mining Scheme", African Journal of Computing & ICT, vol. 5, no. 2, 2012 [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.411.3403&rep=rep1&type=pdf. [Accessed: 08- Feb- 2016].

[9] S. Simmons, D. Edwards, N. Wilde, J. Just and M. Satyanarayana, "Preventing Unauthorized Islanding: Cyber-Threat Analysis", 2006 IEEE/SMC International Conference on System of Systems Engineering, pp. 5, 24-26 [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=165229&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1652294. [Accessed: 11- Feb- 2016] .

[10] I. Ionita and L. Ionita, "An agent-based approach for building an intrusion detection system",RoEduNet International Conference 12th Edition: Networking in Education and Research, pp. 1-6, 26-28, 2013 [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6714184. [Accessed: 11- Feb- 2016].

[11] 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. International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015 36

[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. Ondrej, T. Vollmer, M. Manic, (2009) "Neural Network Based Intrusion Detection System for Critical Infrastructures", Proceedings of International Joint Conference on Neural Networks, pp. 1827 1834.

[15] F. Barika, K. Hadjar, N. El-Kadhi, (2009) "Artificial neural network for mobile IDS solution", Security and Management, pp. 271–277.

[16] S. Mabu, C. Chen, L. Nannan, K. Shimada, K. Hirasawa, (2011) "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol.41, No.1, pp.130-139.

[17] Y. P. Zhou, (2009) "Hybrid Model based on Artificial Immune System and PCA Neural Networks for Intrusion Detection", Asia-Pacific Conference on Information Processing, Vol. 1, pp. 21 – 24.