IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

Artificial Intelligence in Cyber Security

Ms. Divya Shinde[1], Mrs. Ashwini Sheth[2], Mrs. Gauri Malwadkar[3]
Student, M.Sc.IT.[1]
Assistant Professor, Department of I.T[2,3]
I.C.S. College, Khed, Ratnagiri

Abstract: *Without significant automation, individuals will not be able to handle the complexity of the operations and the amount of information to be used to protect cyberspace. However, in the case of traditional, fixed technology and software implementations, it is challenging to construct the hard wired logic of decision-making in order to effectively protect against security risks. This condition can be remedied through machine simplicity and the learning method in Artificial Intelligence (AI).*
This paper provides a brief overview of the AI implementations of various types of cybersecurity using artificial technologies. It also evaluates the prospects for increasing the cybersecurity capabilities by improving the defence mechanism. We may conclude that valuable applications are already available after reviewing the current artificial intelligence software for cybersecurity. First, they are used for protecting the periphery as well as many other cybersecurity areas using neural networks. However, it was evident that certain cybersecurity problems will only be effectively solved if artificial intelligence approaches were deployed. For instance, in strategic decision making, comprehensive information is very important. Logical decision assistance is also one of the yet unanswered cybersecurity issues.
As cyber threats become more sophisticated, the relationship between AI and cybersecurity is becoming increasingly important in strengthening digital defences.

Keywords: Intelligent Agents, Artificial Intelligence, Smart Cyber Security methods, Neural networks

REFERENCES

[1] Smart technology / applications in cyber security. (n.d.). Retrieved August 14, 2020, from https://www.researchgate.net/publication/333477899_Use_of_Artificial_Intelligence_Techniques_Applications_in_Cyber_Defense.
[2] Ahmad, I., Abdullah, A. B. and Alghamdi, A. S. (2009). We apply artificial neural networks to detect DOS attacks. SINand#039;09 - Proceedings of the Second International Conference on Information and Network Security, 229–234. https://doi.org/10.1145/1626195.1626252.
[3] Bai, J., Wu, Y., Wang, G., Yang, S.X. and Qiu, W. (2006). A new recognition model based on multiple self-organizing maps and key component analysis. Computer Science Class Notes (including Artificial Intelligence subsections, Class Notes, and Bioinformatics Class Notes), 3973 LNCS, 255-260. https://doi.org/10.1007/11760191_37.
[4] Bitter, C., North, J., Elizondo, D. A., & Watson, T. (2012). An introduction to the use of neural networks for network intrusion detection. Research in Computer Science, 394, 5-24. https://doi.org/10.1007/978-3-642-25237-2_2.
[5] Carrillo, F.A.G. (2012). Can technology replace teachers in educational relationships with students? Procedia - Theory and social behavior, 46, 5646-5655. https://doi.org/10.1016/j.sbspro.2012.06.490.
[6] Chang, R.I., Lai, L. Bin and Kouh, J.S. (2009). Network intrusion detection using signal processing using query-based pattern filters. Eurasip Journal on Advances in Signal Processing, 2009. https://doi.org/10.1155/2009/735283.
[7] Chatzigiannakis, V., Androulidakis, G. and Maglaris, B. (2004). An example of distributed intrusion detection using security agents. HP OpenView University Association, June 2014.
[8] Chmielewski, M., Wilkos, M., & Wilkos, K. (2010). Building a Multi-Enterprise Environment for Military Decision Support Tools Using Semantic Services. Computer Science Class Notes (Including Artificial Intelligence Subseries Class Notes and Bioinformatics Class Notes), 6070 LNAI (PART 1), 173-182. https://doi.org/10.1007/978-3-642-134807_19.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

[9] Corral, G., Llull, U. R., Herrera, A. F., Administrado, H., Ignasi, S. me Llull, U. R. (2007). Innovations in Hybrid Intelligent Systems {--} Articles of the II International Workshop on Hybrid Artificial Intelligence Systems (HAISand#039;07). 44/2008 (Pipiri 2014). https://doi.org/10.1007/978-3-540-74972-1.

[10] Feyerisl, J. and Aickelin, U. (2009). S Elf - Management M Aps. 1.-30. Akuhata.

[11] Ghosh, A.K., Michael, C., e Schatz, M. (2000). An intruder detection system based on the characteristics of the project. Informatics class notes (including the subseries of Artificial Intelligence Lecture Notes and Bioinformatics Lecture Notes), 1907, 93-109. https://doi.org/10.1007/3-540-39945-3_7.

[12] Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T. and Dehmeshki, J. (2012). An automated approach to learning and refining type 2 Gaussian phase membership functions for pulmonary CAD classification systems. IEEE Transactions on Fuzzy Systems, 20(2), 224–234. https://doi.org/10.1109/TFUZZ.2011.2172616.

[13] iOS Press. (n.d.). Retrieved on October 14, 2020 from https://www.iospress.nl/book/algorithmsand-architectures-of-artificial-intelligence/.

[14] Kotenko, I. and Ulanov, A. (2007). A multi-agency framework for benchmarking adaptive defense performance against cyberattacks. Computer Science Class Notes (Including Artificial Intelligence Class Notes Subseries and Bioinformatics Class Notes), 4476 LNAI, 212-228. https://doi.org/10.1007/978-3-540-72839-9_18.

[15] Kotenko, I. V, Konovalov, A., and Shorov, A. (2010). Client modeling and botnet modeling and botnet protection. In The Internet War Forum (pp. 21-44). http://ccdcoe.org/229.html.