World of Science: Journal on Modern Research Methodologies

Volume 2 Issue 6, Year 2023
ISSN: 2835-3072
https://univerpubl.com/index.php/woscience

Technology to Defend against Cyber Attacks with the Help of Artificial Intelligence

Anirban Chakraborty
Research Scholar, Department of Artificial Intelligence, Agartala, India

Article Information

Received: April 23, 2023
Accepted: May 25, 2023
Published: June 12, 2023

Keywords: *Cyber security, Artificial Intelligence (AI), Security intelligence, Cyber defence, Denial of Service (DoS), and Self-Organizing Maps (SOM)*

ABSTRACT

Clearly, cyber security is the field that will benefit the most from the introduction of AI. It is difficult to create a defence against powerful system attacks. Utilising artificial intelligence techniques will be of great assistance. Where conventional defence systems may be feeble and sluggish, artificial intelligence approaches may enhance their security programme implementation and provide significantly enhanced protection against a growing number of cyber threats. While AI's information protection policies offer advantages, their use has legitimized concerns and threats. In order to promote more effective cyber protection initiatives, it is necessary to adopt an alternative perspective of cyber earth connections that combines AI with human consciousness, as neither humans nor AI have historically proved to be effective in this particular field. Therefore, it is necessary to employ AI methods with social caution in order to reduce the associated problems and dangers.

1. INTRODUCTION

To ensure consistent and scalable health, the online game's security mechanism must collaborate incessantly with changing participants, threats, and the environment. Cyber fact, regardless of quantity, is distinguishable. As a result of the protection system's fluidity and inability to respond to shifts within its scope, modification methods can be ineffective and cumbersome, even for individual experiences, when used to modify documented assaults.

Due to their adaptable and versatile device behaviour, approaches based on artificial intelligence may assist in overcoming a number of limitations of contemporary information protection techniques. While AI's data security has been significantly improved, you may still be concerned. Many individuals view AI as a growing existential peril to humanity. Similarly, solicitors and scientists are cautious about the position of self-government. AI is capable of focusing on how the mind functions, as well as how humans comprehend, evaluate, and act in an effort to solve a problem. Before this, the end result of this evaluation is used to develop intelligent systems and software [1].

The purpose of this initiative is to emphasise the lack of conventional protection mechanisms as well as the success gained to date with AI-based approaches to information security. In addition, this role reduces the risks and issues associated with this growth by analysing the current state of AI, retaining issues, and forecasting the future.

© 2023 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).



FIG 1 : EVOLUTION OF ARTIFICIAL INTELLIGENCE

2. APPLICATIONS OF AI TECHNOLOGIES

I also described the use of multiple AI techniques to prevent cyber-attacks in this region. As we acquire knowledge, we are preparing for a near future in which we will communicate with a computer that is more intelligent than us. As the approaches continue to generate risks and daily attacks, we must implement AI tactics within our defence framework to identify this specific attack.

A. IMPLEMENTATION OF SMART AGENTS

Smart agents are self-sustaining computer network powers that communicate with one another to transmit information and frequently collaborate on organising and updating the appropriate responses to unforeseen incidents. Intelligent agents are capable of defending against cyber-attacks due to their strength, endurance, and synergistic nature under certain conditions.

Intelligent agents (distributed denial of service) are employed to counter DDoS attacks. After resolving numerous legal and commercial issues, it will be possible to implement a standard of cyber protection that incorporates intelligent (portable) components. The deployment of infrastructures is necessary to support the cyber worker's communications and transportation, but they are inaccessible to adversaries. For the comprehensive organisational representation of cyberspace, a multi-agent protocol is presently proposed, such as neural network intrusion detection and combined MultiAgent Strategies. In [3], an intrusion is predominantly identified on a central worker.

B. THE USE OF NEURAL NETWORKS

The invention of Frank Rosenblatt's perceptron in 1957 signified the commencement of a previous neural network; an artificial neuron is referred to as essential neural network ingredients [4]. By utilising modest quantities, perceptions can investigate and solve complex problems. In the neural network are numerous artificial neurons. Neural networks have the advantage of reasoning and deciding significantly simultaneously. They are familiar with the operating level.

© 2023 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).

Their algorithm is optimal for identifying patterns, schemes, and attack reactions [5] and so on. We continue to assist with software and even apparatus deployment. Utilising neural networks, the identification and elimination of intrusion is accomplished [6 10]. They are recommended for use in the recognition of marks, analysis of undead and spam, diagnosis of viruses and laptopworms, and forensic testing [11,13].

Popular in cyber defence is the neural network's speed when implemented on hardware or as a graphics processing feature. Various recent advancements in the revolutionary 3G neural networks of the neural network – in these particular biological neurons – have enabled neural nets to emulate domain opportunities more prudently. Field Programmable Gate Arrays (FPGA) make it possible to swiftly develop neural networks and adapt them to evolving threats.

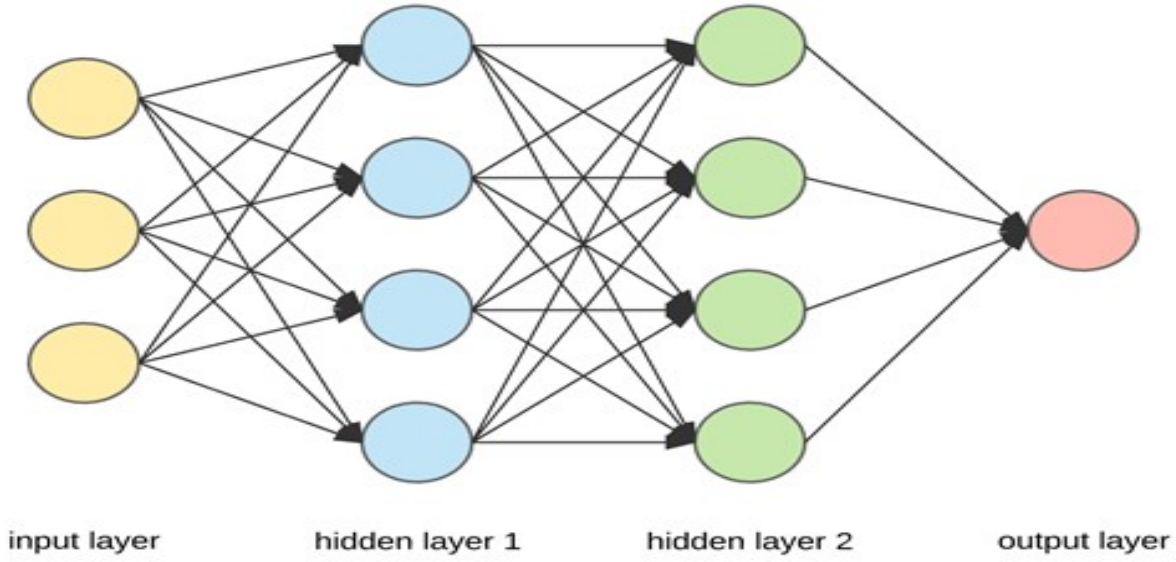


FIG 2: THE NEURAL NETWORKS

C. APPLICATION OF PROFESSIONAL METHOD

Expert phone programme is the most popular AI application. It is a software system that searches for answers to consumer or perhaps an external application's questions regarding the use of finance, scientific research, and cyberspace, as well as the direct application of the service of choice. There are a variety of expert structures, ranging from basic research programmes to integrated models, which are effective and extremely comprehensive for solving complex problems.

A professional information base for a specific application field comprises of a pro method. In reality, it provides an inference mechanism for weakened knowledge and additional information about a situation based on the current comprehension. The expert framework's shell comprises the vacant information base and the deduction motor, which must be assembled prior to use. In addition to experience in client collaboration programmes and various technologies required by hybrid pro frameworks, the professional process shell will be included in the information base software package Professional process shell. The expert method is designed to ensure cyber security. It will aid in implementing protection measures and directing the optimal use of limited resources. The utilisation of specialist approaches for intrusion prevention is established [14, 15].

The expert system's knowledge base, other configurations, and rule sets are crucial for detecting Network intrusion details. As part of the site's system, a database containing the relevant knowledge base contains and displays various network attack characteristics. It is crucial to successfully convey the theory set in real-time data fragments. The rules can also be retrieved from the servers and administered using the programme infrastructure.

© 2023 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).

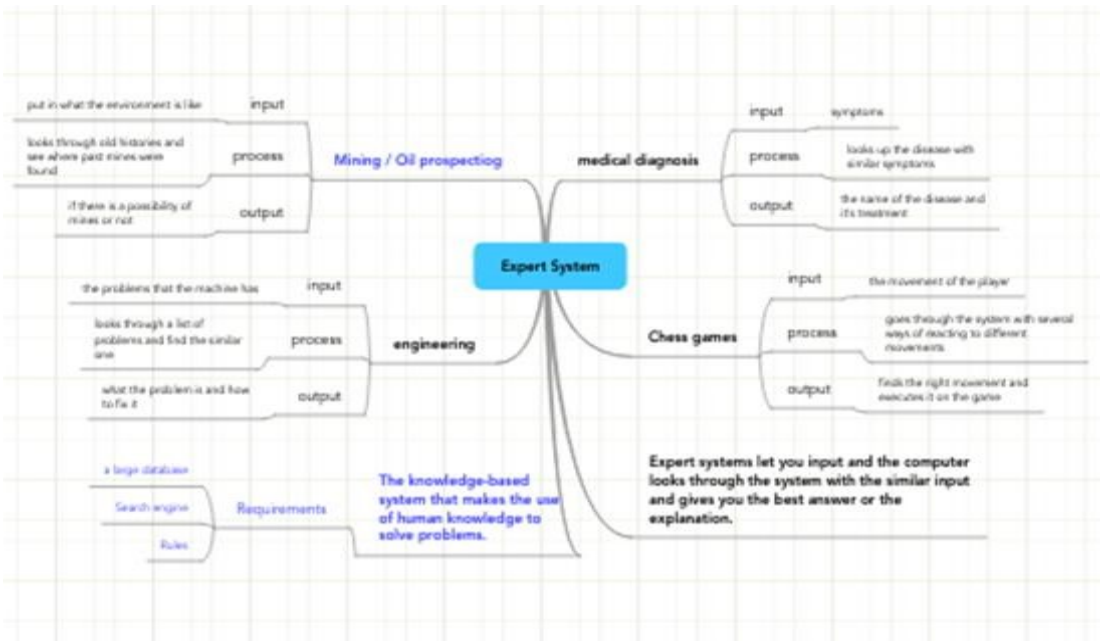


FIG 3: The Expert System

D. IMPLEMENTATION OF DEEP LEARNING

Through machine learning, it is possible to gain brand-new understanding, fresh new expertise, and even enhanced methods for enhancing existing data. The difference between a bachelor's degree and a master's degree would depend on their level of sophistication, from simple parametric learning to complex abstract thought, analogy, concept thinking, and functional learning, grammes and operations. Additionally, monitored and unattended instruction may be utilised.

Unsupervised learning is essential for acquiring vast quantities of knowledge. This is precisely where the cyber security industry can obtain massive records. The concept of data mining was unsupervised AI learning. In certain circumstances, Self-Organizing Maps (SOM) can also be a benefit of neural networks[10, 16, 13, 17].

Learning strategies consist of concurrent algorithms distributed on scalable hardware. Neural networks and genetic algorithms are examples of these learning methods. As demonstrated in [18], fuzzy logic and genetic algorithms are still utilised in risk detection methods. Few systems comparable to [19, 20, 21] have been implemented.

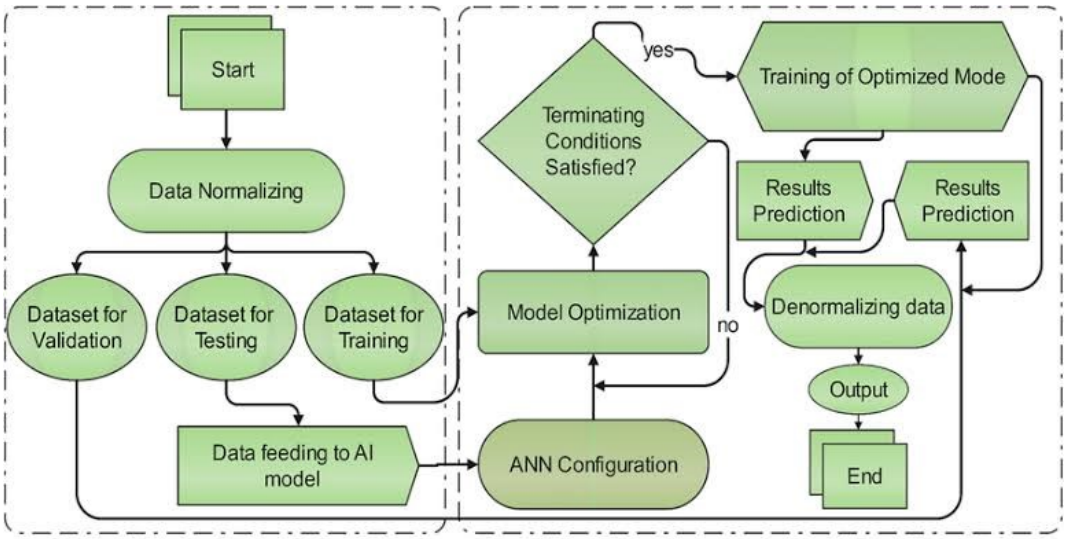


FIG 4: THE DEEP LEARNING PROCESS

© 2023 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).

3. EXAMINATION OF FUTURE ISSUES

If you foresee the potential research, implementation, and growth of cyber-attack protection strategies for AI, you must be aware of the significant gap between accelerated goals and long-term expectations. Many AI techniques are adequate for identifying cyber-attacks, but other actual cyber-attack challenges are typically required for advanced action.

In decision-making, one may observe the application of a variety of distinct criteria for judging competence. Such requirements provide a structured and functional knowledge system for project decision making. The automated information management system provides leaders and policymakers with rapid assessments of the situation, granting them control over C2-level defence.

As has been the case in a number of projects to date, specialist approaches frequently conceal the presence of their technology within the same environment as the safety-planning framework.

As significant bases of expertise are established in the future, expert strategies will produce more complex systems. Significant acquisitions and extensive, scalability-enabled information bases would be necessary to attain this specialised job knowledge. Implementing the professional approach would necessitate additional enhancements: modular apparatus and hierarchical data bases will be incorporated into the professional process.

4. APPLICATION OF AI TECHNOLOGIES AND THEIR BENIFITS

The applications and benefits of AI techniques are summarised in Table 1.

Table.1. AI techniques and their usage

AI Techniques	Usage
Intelligent Operator	Proactive Agent communication language
	Reactive
	Defence against DDoS
	Mobility
Application of Neural Nets	For intrusion detection and prevention system,
	Very high speed of operation,
	For DoS detection,
	For Forensics Investigation
	Warm detection
Application of Expert System	For decision support For Network Intrusion Detection
	Knowledge base
	Inference engine
Application of Learning	Machine learning
	Supervised and unsupervised learning.
	Malware detection, intrusion detection.
	Self-Organizing Maps (SOM)

© 2023 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).

5. CONCLUSION

In addition to computer security, AI is recognised as one of the most significant technological developments of the digital age. The global safety exhibit must be followed by additional approaches, an algorithm, services, and organisations that offer AI-based solutions. Such application structures aspire to be more adaptable, stable, and versatile than conventional data safety approaches, thereby enhancing protection implementation and defending the network against an expanding array of sophisticated cyber threats. Today, the most persuasive and effective AI instruments are deep learning techniques. Among other fields where the most recent innovation is not limited to neural networks, the application of intelligent cyber security technologies is frequently significant. Nobody or AI alone has demonstrated a standard of success in information security in recent years. Despite the significant advancements that AI has made to the cyber-security domain name, the systems are not prepared to change their situation adequately and completely. Also essential is a comprehensive view of the cyber world of partnerships.

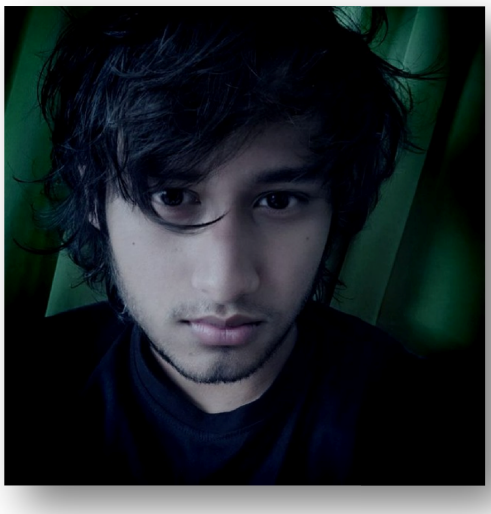
REFERENCES

1. E. Tyugu. Algorithms and Architectures of Artificial Intelligence. IOS Press. 2007.
2. E. Herrero, M. Corchado, A. Pellicer, A. Abraham, “Hybrid multi agent-neural NIDS with MV”.
3. V. Chatzigiannakis, G. Androulidakis, B. Maglaris. A DIS Prototype Using Security Agents.
4. F. Rosenblatt. The Perceptron a perceiving and recognizing automaton.
5. G. Klein, A. Ojamaa, P. Grigorenko, M. Jahnke, E. Tyugu. Enhancing Response Selection in Impact Estimation Approaches
6. J. Bai, Y. Wu, G. Wang, S. X. Yang, and W. Qiu, “A novel intrusion detection model based on multi-layer selforganizing maps and principal component analysis.
7. F. Barika, K. Hadjar, and N. El-Kadhi, “ANN for mobile IDS solution,” in Security and Management.
8. D. A. Bitter, T. Elizondo, Watson. Application of ANN and Related Techniques to Intrusion Detection.
9. R.-I. Chang, L.-B. Lai, W. D. Su, J. C. Wang, and J.-S. Kouh, “Intrusion detection by backpropagation neural networks with sample-query and attributequery,”
10. L. DeLooze, Attack Characterization and Intrusion Detection using an Ensemble of SOM.
11. B. Iftikhar, A. S. Alghamdi, “Application of artificial neural network in detection of dos attacks,”
12. D. Stopel, Z. Boger, R. Moskovitch, Y. Shahar, and Y. Elovici, “Application of artificial neural networks techniques to computer worm detection”.
13. B. Fei, J. Eloff, MS Olivier, H. Venter. The use of selforganizing maps of anomalous behavior detection in a digital investigation. Forensic Science International, v. 162, 2006, pp. 33-37.
14. D. Anderson, T. Frivold, A. Valdes. Next-generation intrusion detection expert system (NIDES).
15. TF. Lunt, R. Jagannathan. A Prototype Real-Time Intrusion-Detection Expert System. Proc.
16. J. Bai, Y. Wu, G. Wang, S. X. Yang, and W. Qiu, A novel intrusion detection model based on multi-layer selforganizing maps and principal component analysis.

© 2023 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).

17. V. K. Pachghare, P. Kulkarni, D. M. Nikam. Intrusion Detection System using Self Organizing Maps.
18. R. Hosseini, J. Dehmeshki, S. Barman, M. Mazinani, S. Qanadli. A Genetic Type-2 Fuzzy Logic System for Pattern Recognition in Computer Aided Detection Systems.
19. Naba Suroor and Syed Imtiyaz Hassan, "Identifying the factors of modern day stress using machine learning", International Journal of Engineering Science and Technology, vol. 9, Issue 4, April 2017, pp. 229-234, eISSN: 0975–5462, p-ISSN: 2278–9510.
20. Syed Imtiyaz Hassan, "Designing a flexible system for automatic detection of categorical student sentiment polarity using machine learning", International Journal of u- and e-Service, Science and Technology, vol. 10, no.3, Mar 2017, pp. 25-32, doi: 10.14257/ijunesst.2017.10.3.03, ISSN: 2005-4246.
21. Syed Imtiyaz Hassan, "Extracting the sentiment score of customer review from unstructured big data using Map Reduce algorithm", International Journal of Database Theory and Application, vol. 9, issue 12, Dec 2016, pp. 289-298, doi:10.14257/ijdta.2016.9.12.26, ISSN: 20054270.

AUTHOR INFORMATION



Name: Anirban Chakraborty

Degree: B.Tech, Computer Science and Engineering, Lovely Professional University

MTECH, Artificial Intelligence, Lovely Professional University

Currently: Research Scholar, Artificial Intelligence

Location: Agartala, India

Email : anirforyouall@gmail.comm

© 2023 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).