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

IJIEMR Transactions, online available on 11th Jan 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 01

DOI: 10.48047/IJIEMR/V12/ISSUE 01/73

Title Use of Artificial Intelligence in the field of cybersecurity - An Overview

Volume 12, ISSUE 01, Pages: 785-794

Paper Authors
Kayala Manogna, Dr. D. Aruna Kumari

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

Use of Artificial Intelligence in the field of cybersecurity - An Overview

Kayala Manogna *1, Dr. D. Aruna Kumari *2
[1]PG Student, Computer Science and Engineering, Vidya Jyothi Institute of Technology, VJIT, Aziz Nagar, Hyderabad, Telangana, India.
[2]Professor and Head of the Department, Computer Science and Engineering, Vidya Jyothi Institute of Technology, VJIT, AzizNagar, Hyderabad, Telangana, India.

Abstract

As the development in technology continues, the dependency on it has also been increased drastically in our day to day life. For any task, be it as simple as writing notes to performing sensitive financial transactions, we have started depending on internet and technology for everything. Due to this, there is a need to employ security measures to safeguard the vast amounts of data from being breached. But just as better measures are being employed, cyber attackers are finding out different new ways to infiltrate and breach the data, on top of the already existing security measures. Using artificial intelligence models and techniques in cybersecurity have shown to be effectively counter the threat of cyber-attacks. Here we have discussed regarding use of AI in the field of cybersecurity, various methods that can be employed, the advantages and disadvantages. One must have sound knowledge of the existing methodologies employed in the field of cyber security to better understand what kind of models must be developed and employed in cyber security for advancing in protection and security against cybercrimes.

Keywords – Artificial Intelligence, Cybersecurity, Cyber-attacks, Cyber Crimes.

Introduction

Cybersecurity is the practice of securing and providing protection to devices such as computers, networks, and data, from being accessed and used illegally. It can be described as a set of methodologies employed to protect sensitive data (personal, governmental, etc.) from being accessed and used by cyber criminals. If the cyber criminals get the access to that sensitive data, it might lead to a huge loss. Hence, various methodologies exist to protect the data and devices.

For instance, Internet is something which is extensively used, so there is a lot of data transfer which is very sensitive and enormous. Due to this, the amount of cyberattacks which occur is very huge. There are security measures being implemented for it, but attackers are also using advanced ways of breaking in, making the cyberattacks very sophisticated and advanced. Due to this, the traditional methodologies implemented for cybersecurity are becoming outdated and there is a need for advanced methodologies. Cyber threats will continue to rise, even as they are identified and solutions are developed with the help of various technologies.

This is where artificial intelligence comes in, which can be utilized in the field of cybersecurity. AI is the branch of computer science used for producing automatic security systems which are intelligent. The primary purpose of artificial intelligence here is for training models or a computer to think, learn, work, perform and behave like human beings.

AI possesses powerful data analytic capability and it can be used to study vast amounts of electronic data with agility and effectiveness. AI system possesses the capability to predict future cyber attacks based on past threats, even if the threats change, making AI very unique. Due to these abilities of artificial intelligence, it can be considered and employed for cyber security.

AI has many branches like Neural network, ML, Data Mining, Deep learning, expert systems, etc. Each of them is used in cyber security and also has a specific application in cybersecurity.

Literature Survey

As the cyber-attacks have become more sophisticated, Artificial Intelligence has become a crucial technology in the field of cyber security. Sherally et al., (2020) has described that artificial Intelligence system has the potential to foresee cyber-attacks in the future based on past occurrences, even if the threats change, as AI model could be used to train models or computers to think, learn, work, perform and behave just as human beings. The AI methodologies propose a range of intelligent behaviour, from how machines can think to acting humanly.

Cyberattacks not only disrupts data and computer, but also create a threat upon human well-being. Due to this, there is an increase in need to employ better methodologies against cyberattacks. Using Artificial Intelligence has given a better way of overcoming such attacks by training and predicting cyberattacks before they can occur, so better precautions can be taken so that attack does not happen and no negative impact can be encountered.

An extensive review of cyber threats and elucidations has been provided by Sherally et al., (2020); particularly it has been expressed how cyber attacks can be launched on different network stacks and applications, along with their impact [1].

Ishaq Azhar et al., (2020) has described that AI has swiftly become a must have instrument for improving the effectiveness of information security teams. Human beings are no longer adept of sufficiently securing an enterprise-level attack surface, and AI provides the much needed analysis and threat detection that can be employed by security professionals to reduce the chance of a breach and betterment of the security structure for the organization.

As further technology is integrated into our daily lives, the effect of AI on our lives will persist to increase. Even though there are drawbacks of using Artificial Intelligence in cybersecurity such as to develop a sustainable artificial intelligence system organizations would need a lot of resources and finances, the advantages of using AI is a lot more than the disadvantages, and the need for a newer methodology along with the advantages of using AI has made use of AI in the field of cybersecurity a better approach.

Muhammad Shoaib et al., (2021) has elaborated that the use of traditional security methodologies have become outdated, as newer and more potent cyberattacks have been seen to come into play, the need to use an effective and efficient methodology such as Artificial intelligence has come into use for cybersecurity. Artificial Intelligence has various branches such as deep learning and Machine learning, two latterly developed fields of Artificial Intelligence have proved much efficient in fighting cyber attacks. Some of the techniques of AI models used in cybersecurity are neural networks, deep learning, expert systems, machine learning, and data mining. Each technique has various distinguishable applications in cybersecurity. Some of such applications are Denial-of-service (DoS) detection, network intrusion detection, Inference engine, etc.

As previously mentioned, use of artificial intelligence has both advantages and disadvantages, but as we are in need of a better cyber security, we have decided to consider AI to be integrated with cybersecurity.

Ayodeji et al., (2020) has described the security and privacy for AI and various disputes which are faced. Increase in use of Artificial intelligence has helped in various ways, be it employing for solving problems or challenges. But one aspect we must keep in mind is a better way of securing the artificial intelligence model. The main security properties are confidentiality, integrity, availability and privacy. An attacker tries to attack these properties, treating them as goals. For instance, to attack confidentiality, the attacker tries to get insights about the working of the model or the dataset and using this information, tries to carry out more advanced attacks. The Artificial intelligence system must have less to none vulnerabilities so that there will be a decreased chances of a successful attack.

Feng Tao et al., (2021) has briefed that as cybercrimes are evolving, it has become complex, and hence cybersecurity approaches need to become more intelligent. With that the defence mechanisms must be able to take decisions that can be employed effectively on various attacks. For this to be achieved, one must extensively know the cyber security methods in use. Only then artificial intelligence can be used to counter cyberattacks and cybercrimes. One must use efficient and accurate data to train the models so that the occurrence of incorrect results will be reduced (Feng Tao et al., 2021).

Atiku et al., 2020 has specified that with efficient and swift technology being employed to operate artificial intelligence system, they are also doubtlessly to enhance the security and businesses of customers in cyber space. This was seen to be proven by increasing the deployment of artificial intelligence engines then the conventional engines in cyber security.

Methodologies

There is an increase in cyber threats as the technology has advanced and the usage of internet has increased. It is also predicted this threat will increase a lot in the future. The only available alternative for now is employing artificial intelligence models in the aspect of cyber security.

Now the question arises of how to apply these artificial intelligence models in cyber security. There are various advantageous ways these AI models can be employed which has various benefits. Some of such benefits are:

1. Traditionally the technology was focussed and dependent on the past data on only recognisable cyber-attacks. If a new cyberattack is encountered the traditional systems won't be able to detect it. Artificial Intelligence can determine new and complex alterations in attacks. In the future, AI systems will become sensitive to detect new patterns. The study and tailoring for Artificial Intelligence system is loftier and can detect faster and more accurate operations. This ability of AI systems is more important when cyber attacks are becoming more sophisticated and cyber criminals are coming up with advanced procedures (Muhammad Shoaib etal., 2021).
2. Using Artificial Intelligence, we can handle large amounts of security data (Truong et al., 2020). It is because Artificial Intelligence includes a self-sufficient system that can determine attacks and counter accordingly. The number of data leaks occurring every day is huge, hence handling it manually id very difficult, so this feature of AI to detect and respond to attacks has reduced a lot of workload (Muhammad Shoaib et al., 2021). Using AI, vast amounts of data can

be easily narrowed down in a matter of milli seconds, as an outcome of which the business can easily detect and also recuperate from threat quickly (Bhutada et al., 2020).

3. Application behaviour and regular network traffic is studied by Artificial Intelligence security systems over time. In this way determining the threats over a period of time, Artificial Intelligence makes a standard of what are the normal patterns (Muhammad Shoaib et al., 2021). So if any deviation is found from the standard pattern, Artificial Intelligence security system will locate it.

AI methods in cyber security:

Neural Networks, deep learning, Expert Systems, ML, and Data Mining are a couple of the Artificial Intelligence models that can be employed to productively handle cyber attacks and threats (Muhammad Shoaib et al., 2021).

1. Artificial Neural Network (ANN)

Artificial Neural Network or ANN mimics neurons in the form of a mathematical equation where the model reads extensive samples to generate a target value. ANN's are highly adept to know, learn and resolve the problems in different areas. It's also adept to solve noisy and incomplete data samples. ANN's have the capacity to learn from previous network activities to terminate threats that could occur in the future. Using formerly transferred data over the network, ANN's can find out normal and abnormal network patterns (Atiku et al., 2020).

Deep Neural Networks (DNN), which is an advanced form of ANN, not only safe guards the security system from cyber attacks, but also predicts such attacks can or will occur in the future (Hinton et al., 2006).

2. Expert System

In Artificial Intelligence, expert system is an implementation that helps a person to decide. Expert system modelling has various applications in medical diagnosis, finances, and cyber space. There are 2 kinds of approaches here, case based and rule based (Muhammad Shoaib et al., 2021).

Case based approach is where for every problem, based on previously occurred similar cases and solutions a new solution is determined.

In rule based approach, based on the condition evaluation to analyze the problem, the action to be taken is determined.

Intelligent Agents

Intelligent agents (IAs) are self-controlled systems with internal decision making methodology and a specific objective. It assesses threats through sensors and monitors the domain through actuators.

Intelligent agents are adaptive, that is they can learn from their environment and respond accordingly.

Machine Learning

Machine learning or ML is a branch of AI that handles regarding teaching machines to learn new things and make various decisions based on data with the help of various mathematical algorithms. There is a concept called Deep learning where one can train a system to simulate human behaviour. Both Machine Learning and Deep learning have seen to be effective in the field of cyber security (Muhammad Shoaib et al., 2021).

Search

It is a day to day problem solving methodology applied subconsciously by everyone. When putting in the search strategy, basic knowledge about it is needed prior a general search algorithm is performed. Some or the other form of search algorithm is built into approximately every intelligent program, and it's effectiveness hugely impacts the performance of the entire program. A wide range of search methods have been developed which takes into account the specific information related to issues of inquiry (Atiku et al., 2020).

Bio inspired computation methods

Bio-inspired computing is a branch of AI which is being predominantly studied since the latest times. It consists of smart algorithms and techniques that mimic the bio-inspired behaviours and attributes to define a broad spectrum of sophisticated academic, as well as real environment problems (Atiku et al., 2020).

Techniques like Ant Colony Optimization (ACO), Evolution Strategies (ES), Artificial Immune System (AIS), Particle Swamp Optimization (PSO), and Genetic Algorithms (GA) are biologically inspired techniques commonly employed in the field of cyber security (Atiku et al., 2020).

The applications of bio-inspired techniques in the field of classifying of computer malwares have gained increasing acceptancy among scientists. These techniques were primarily employed to optimise features and parameters for the classifiers.

Conclusion

Although there are various benefits of employing AI methodologies in the field of cybersecurity, there are also various drawbacks for it. For instance, training a model would require a lot of precision and resources to work correctly. Acquiring a dataset which can be employed will be very huge and hard to acquire. It also demands a lot of time and financial resources.

The kind of data and from where it is acquired also matters. Data must be accurate else there will be a scope for false positives, which is not ideal. Another drawback is if Artificial intelligence is itself being used by cyber attackers in sophisticated cyber assaults. Though this can be encountered, looking at the benefits AI is providing in the field of cyber security, AI being used for cyber-attacks can be overlooked.

Here in the paper, we have briefed regarding the idea of using AI in field of cybersecurity, the benefits, advantages, drawbacks, basic models of AI that can be employed in cybersecurity. AI is the best counter measuring and combating various cyber-attacks. Despite the drawbacks of AI in cybersecurity there is still a lot of scope for it in the field of cybersecurity.

References:

[1]Sherally Zeadally, Erwin Adi, Zubair Baig, Imran A. Khan, “Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity”, IEEE Access, Volume 8, 23817, 2020.

[2]Muhammad Shoaib Akhtar, Tao Feng, “An overview of the applications of Artificial Intelligence in Cybersecurity”, EAI Endorsed Transactions on Creative Technologies, Volume 8, Issue 29, 2021.

[3]Ishaq Azhar Mohammed, “Artificial Intelligence for Cybersecurity : A systematic mapping of literature”, International Journal Of Innovations In Engineering Research And Technology [IJIERT], Volume 7, Issue 9, 172, 2020.

[4]Ayodeji Oseni, Nour Moustafa, Helge Janicke, Peng Liu, “Security and Privacy for Artificial Intelligence: Opportunities and Challenges”, J. ACM, Volume 37,

111, 2020.

[5] Feng Tao, Muhammad Shoaib Akhtar, Zhang Jiayuan, "The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey", EAI Endorsed Transactions on Creative Technologies, Volume 8, Issue 28, 2021.

[6] Atiku, S.B., Aaron, A.U., Job G.K., Fatim, S., & Yakubu, I.Z., "Survey on the Applications of Artificial Intelligence in Cyber Security", International Journal of Scientific and Technology Research, volume 9(10), 165, 2020.

[7]Bhutada, S., & Bhutada, P. "Application of Artificial Intelligence in cyber security". International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), volume 5(4), 214, 2018.

[8]Hinton G. E., Osindero S., & Teh Y. W. , "Fast learning algorithm for deep belief nets", Neural computation, Volume 18, 1527, 2006

[9]Truong T. C., Diep Q. B., & Zelinka I. "Artificial intelligence in the cyber domain: offense and defense", Symmetry, volume 12(3), 410, 2020.

[10] Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V ,"Artificial intelligenmce and cybersecurity : Past, present and future", Springer, 351, (2020).

[11] Tyugu, E. "Artificial intelligence in cyber defense", IEEE, 1, 2011.

[12] S. Rubin, """Knowledge based programming for cyber security solution", The open artificial intelligence journal, volume 5, 1, 2018.

[13] C. Tschider, "Regulating the IoT : Diacrimination , privacy, and cyber security in the Artificial intelligence age", SSRN Electronic journal, 2018.

[14] Naveed Akhtar, Ajmal Main, "Threat of adversarial attacks on deep learning in computer vision a survey", IEEE Access, volume 6, 14410, 2018.

[15] Z. Siddiqui, M. S. Hussain, S, Yadav, " Application of artificial intelligence in fighting against cyber crimes a review", International Journal Adv Res Comp Sci, volume 9, 118, 2018.

[16] M.N.O Sadiku, O. I Fangbohungbe, S. M. Musa, "Artificial intelligence in cybersecurity" Int. J. Eng. Res. Adv Tech, Volume 6, 01, 2020.

[17] B. S. Sagar, S. Niranjan, N. Kashyap, D. N. Sachin, "providing cyber security using artificial intelligence a survey", ICCMC, 717, 2019.

[18] R. Nishant, M. Kennedy, J. Corbert, "Artificial intelligence for sustainability : challenges, opportunities, a research agenda", Int. J. Inf. Manage, volume 53, 102104, 2020.

[19] T. Tagarev, "Diligence – a platform for digital transformation,

cyber security and resilience", information security an. International journal, volume 43, 7, 2019.

[20] M. Roopak, G. Yun Tian, J. chambers," Deep learning models for cyber security in iot networks", IEEE 9th annual ccwc, 452, 2019.