STM JOURNALS

International Journal of
Information Security Engineering

Volume 1, Issue 2, 2023
July—December
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Review IJISE

Study of Blended Learning of Artificial Intelligence in Cybersecurity

B.N. Manjunatha[1,*], J. Ananda Babu[2], M.S. Rekha[3], Shreya Kulkarni[4]

Abstract

Nowadays there are huge applications of internet of things, and cyberattacks are causing concern all over world. To avoid cyberattacks, designing cybersecurity approach is today's basic need. Artificial intelligence has appeared as a powerful tool in the domain of cybersecurity and can be tuned to deal with cybersecurity and cyberthreats. Cybersecurity is an incredibly growing field since the past decade, there are many applications based on cybersecurity, eventually threats are accelerating. The paper will deliberate about the utilization of artificial intelligence and implementation in cybersecurity and annotate on the disadvantages.

Keywords: Artificial intelligence, cybersecurity, cyberthreats, block chain

INTRODUCTION

Cybersecurity is important as it encloses everything that relates to safeguard data from cyberattackers who want to steal information and cause harm. The day to-day elevation and development in cybersecurity threats, it is going through problems which would be reduced by affiliation of artificial intelligence (AI) into cybersecurity. AI and machine learning are connected over industries and applications as there is increase in computing power and data collection. With machine learning and AI, we can deal with the vast measure of information, the information can be obtained within a blink of an eye, which will help the organization to associate and recover from security threats as shown in Figure 1 [1].

***Author for Correspondence**
Manjunatha B.N.
E-mail: manju.master@gmail.com

[1]Associate Professor, Department of Computer Science and Engineering, R.L Jalappa Institute of Technology, Doddaballapur, Karnataka, India
[2]Associate Professor, Department of Information Science and Engineering, Malnad College of Engineering, Hassan, Karnataka, India
[3]Assistant Professor, Department of Computer Science and Engineering, R.L. Jalappa Institute of Technology, Doddaballapur, Karnataka, India
[4]Student, Department of Computer Science and Engineering, R.L. Jalappa Institute of Technology, Doddaballapur, Karnataka, India

Received Date: July 20, 2023
Accepted Date: July 30, 2023
Published Date: August 23, 2023

Citation: B.N. Manjunatha, J. Ananda Babu, M.S. Rekha, Shreya Kulkarni. Study of Blended Learning of Artificial Intelligence in Cybersecurity. International Journal of Information Security Engineering. 2023; 1(2): 1–6p.

LITERATURE SURVEY

1. *Machine learning techniques in cybersecurity: an overview.* This provides a summary on how AI and machine learning can be used to identify the hostile events and threats.
2. *Artificial intelligence and machine learning in cybersecurity: an overview.* This tells us how AI is implemented in cybersecurity.
3. *Cybersecurity threat detection using machine learning techniques: a comprehensive review.* This discusses in detail about the different machine learning techniques that are used in identifying threats.
4. *Applications of artificial intelligence and machine learning in cybersecurity.* It lets us know us about the applications of AI and machine learning which is included in cybersecurity.
5. *Artificial intelligence in cybersecurity: a systematic literature review.* Research on applications of AI, the current trends.

Figure 1. Artificial intelligence in cybersecurity.

INTERACTION OF ARTIFICIAL INTELLIGENCE WITH CYBERSECURITY

AI is used to make the structure of a computer in a manner that, where computer is controlled by a robot or any other software brilliantly. AI helps us know how humans think, it is made in such way that machines can know what type of thinking is going on in humans. So, the software is developed more proficiently than humans, to detect the threats easily and solve them accordingly.

Surfacing of Artificial Intelligence

AI can examine a large amount of data; it will allow us to know and identify the threats at the earliest. Many IT companies have already involved this to reduce the threats. Using many machines learning algorithms, it can recognize the patterns and the other anomalies which humans fail to notice. It will also analyze human behavior; AI can detect and will prevent some insider threats which may be found. It will make us learn from the threats which are already committed so that we can learn about improving self, which leads to the defense system and also the increase in security.

AI will work as a genius where you can prepare the machine learning algorithms and also implement programs based on AI. It will be more alert when compared to normal worker. With AI, the work done by 10 employees can be accomplished in much less time. AI will not at all get extremely tired as shown in Figure 2 [2].

Figure 2. Artificial intelligence shaping cybersecurity arms.

Implementation of Artificial Intelligence in Cybersecurity

When we speak about AI usage in cyberthreats, AI plays a crucial role to detect the problem to solve it. As AI will reduce the time by reading data, which is structured or unstructured, it also helps in speech recognition and patterns. AI will maintain the information which is confidential. Many people try to access the data and devices where it is security is slack and where cracks appear without notice [3]. So AI makes sure if the people are getting any emails, which may be spam, so nowadays people are being told to do all the required authentication procedures.

Block Chain

The amazing growth in cryptocurrency like Bitcoin has led to transformation in the payment system, has been the advantage for easier transaction and payment cannot be reversed easily. Medical records are now checked by several authorities. Experts make sure to increase the security to prevent cyberattacks as shown in Figure 3.

Botnets

Group of enormous number of objects contaminated by the same malware (i.e., internet of things devices, servers, computers, cell phones with internet). It is identified on the basis of pattern recognition as shown in Figure 4.

Figure 3. Artificial intelligence in blockchain.

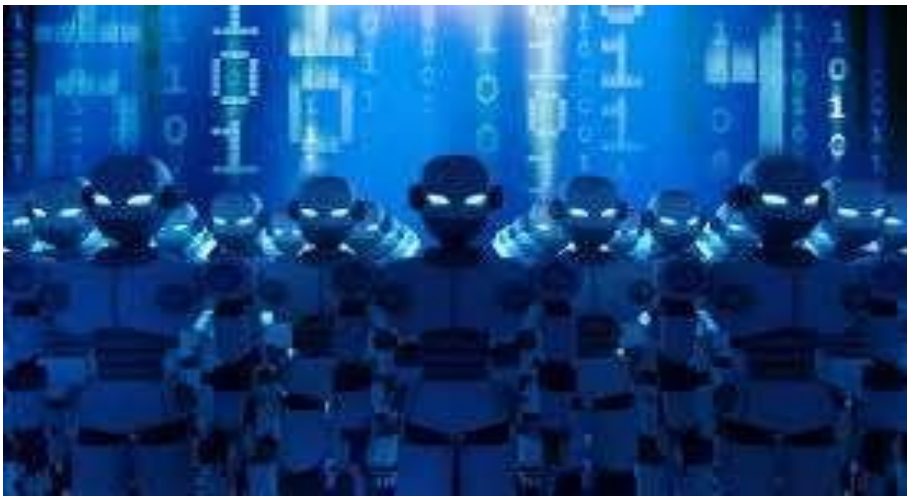

Figure 4. Artificial intelligence in botnets.

WORKING OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

The flowchart in Figure 5 tells us about the working of AI in detecting the threat earlier so that we can take preventive measures to avoid the threat. AI is further divided into narrow and general AI. Furthermore, we make use of the machine learning concepts which is based on different algorithms making use of it will help in anomaly detection, network traffic analysis, and threat intelligence will detect the unusual patterns of packets sent and analyze the threat. This will play a crucial role in detecting the threats and help the enterprises and the people to safeguard their resources and data from the hackers. Here, the supervised type of machine learning consists of large amount of data and if the data is not found with the usage of machine learning algorithms, it will help to detect the threats and also the inconsistency.

Large data will further find the software, which is made of viruses, worms, trojans and detect the software which will damage the system. It will find the information provided which is irrelevant so in this it will work with the usage of concepts provided by artificial intelligence.

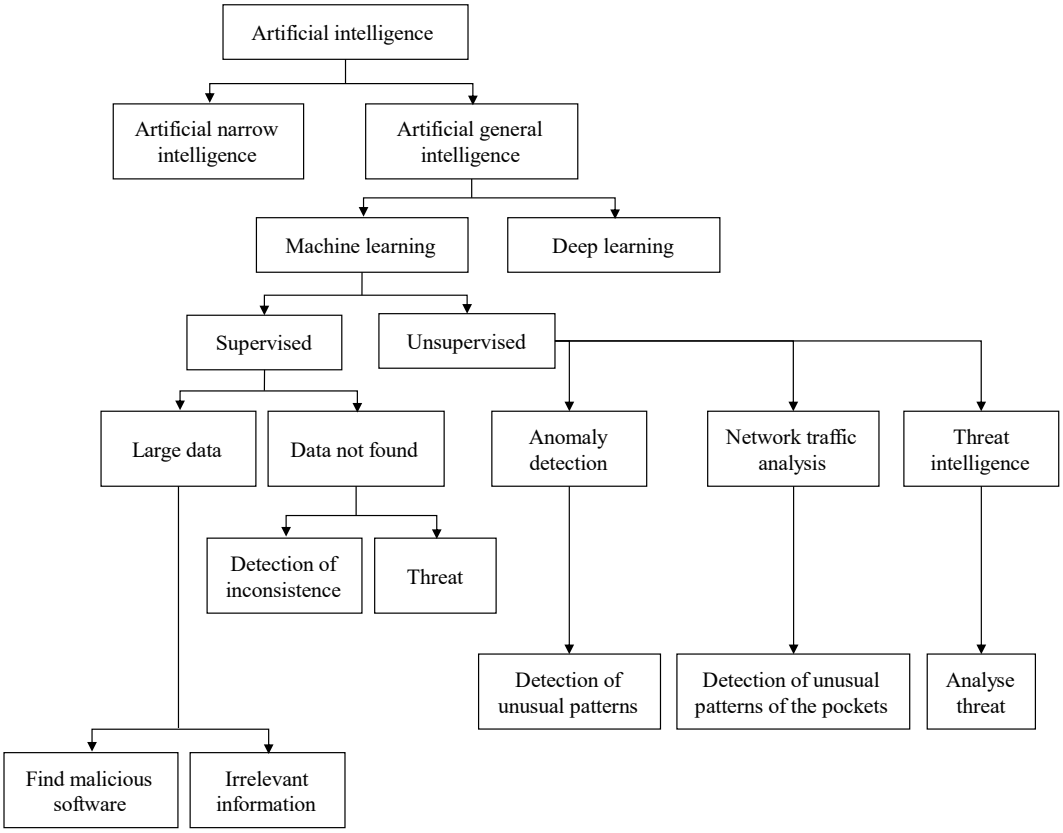

Figure 5. Flowchart of working of artificial intelligence in cybersecurity.

THREATS IN CYBERSECURITY

Threats in cybersecurity mainly focus on damaging the security of the data and the software available and the networks. There are different types of threats in cybersecurity. It is affecting the privacy of the people by attacking their personal data and accessing it without the knowledge of the people.

1. *Malware:* It is the software, which is created and implemented to damage the system. It is mainly made of worms, viruses and many others which will in turn affect the data which is available in the system.
2. *Phishing:* This is the method used by the cyberpunks to attack on the mails of the users by sending spam mails which allows the attackers to access confidential data like bank details, passwords, or debit or credit card details.

3. *Denial-of-service:* This type of attack is mainly to extract money from the public. The attack may be from one person or a group of people, and it is depicted to network with traffic which is intended for not giving access to users.
4. *Man-in-the-middle:* It occurs when an attacker interrupts the conversation between two people where the distraction is done.
5. *Insider threats:* The threat occurs by the people who have legal access to the information provided by the enterprises. It may be from individuals who are working for the company, who take the advantage and misuse their access.

KEY CHALLENGES

1. *Data privacy:* The usage of AI will ensure the privacy of information. The data available may be of different types, it may include sensitive information, personally identified data, etc.
2. *Adversarial machine learning:* Cyberpunk can use this technique to access information and can convert it into harmful files. This can affect the security provided by the AI, when it is not identified.
3. *Complexity:* The solutions provided by AI are complex to build, implement, and manage. So, the need of experts is necessary to work with these tools.
4. *Scalability:* AI needs more resources and components; cloud is needed to store the data so the enterprises should provide capital for such resources.
5. *Human error:* Humans can make errors in developing the algorithms and implementing them in the AI technologies.
6. *Interoperability:* As different tools are present, they have different methods for the particular tasks which may indeed affect the transfer of information from one source to another, which may affect the enterprise security system.

Advantages of Artificial Intelligence in Cybersecurity

1. *AI is capable of handling large amounts of data:* In companies, a lot of information exchange is done between customers and the organization on a daily basis constantly. The information should be kept safe from harmful persons and software [4, 5].
2. *Duplicative processes:* Attackers will adapt different approaches to reduce this if a person is assigned the work, he may not work with it properly and may lead to risk to the network [6, 7]. AI takes care of these things and will give cybersecurity.
3. *Time to detect threats is increased:* To keep the network safe in the company, the first step should be identifying threats. It will be ideal if we identify the dishonest data. It will protect our network from lasting damage. Implementation of AI in cybersecurity will detect the risks earlier and the operations on security will get easy [6, 8].
4. *Authenticity protection:* There will be user accounts from most of the websites where users have to login to access the services. For identification, different methods are used like face recognition, CAPTCHA, and fingerprint recognition. By this process we can get to know whether the login procedure done is authorized or not.

Disadvantages of Artificial Intelligence in Cybersecurity

1. *Increase in cost:* The cost of the services provided by AI is high due to which everyone cannot easily access it..
2. *Effect of cybercrisis:* The information and the privacy of the people is not so safe. The cyberterrorists are easily accessing the information, can trace the location if the precaution is not taken at the right time.
3. *Supervising the individual:* AI is nowadays included in every aspect of life where it guides humans to work.
4. *Increase in unemployment:* AI is now considered as hazard as the work of humans is replaced by the machines due to which the work is done efficiently but people are getting unemployed.
5. *Not everyone is familiar with AI:* Some of the people do not want to adopt new automation tools and learn them.

FUTURE ASPECTS

AI plays a crucial role in cybersecurity. Using advanced tools like AI, machine learning, and automation will develop cybersecurity. As it detects the threats and responds to them earlier to prevent the threats from harm for long time. Nowadays as enterprises expand vigorously, they will get to know about the problems they are overcoming. Research and information will acknowledge that disbursement of cybersecurity will enlarge in the upcoming days. Usage of blockchain automation will also help in businesses from the heavy industries, in mining, in driving the consciousness of the shareholders, and also the sustainable goals of the company. Banks and financial institutions make the usage of digital crypto currencies, and also encouragement in digitalizing the payments of bills to cooperate in the reduction of fraud and identity theft.

CONCLUSION

In this paper, we have learnt about AI and the emergence of the AI in cybersecurity, its various advantages and how the threats can be reduced. Key challenges faced by AI in cybersecurity and the flowchart how the AI can be used in cyberthreats detection using the algorithms and concepts are presented. The types of cyberthreats are discussed so that users get awareness of these threats so that they can implement the security to their data for the safety. Though there are some disadvantages, AI has a crucial role in cybersecurity. To overcome the drawbacks, AI will help to advance cybersecurity.

REFERENCES

1. Welukar JN, Bajoria GP. Artificial intelligence in cyber security – a review. Int J Sci Res Sci Technol. 2021; 8 (6): 488–491..
2. Podishetti J, Anjaiah K. Role of artificial intelligence in cyber security. Int J Res Adv Computer Sci Eng. 2017; 3 (3): 57–64.
3. Ghosh AK, Michael C, Schatz M. A real-time intrusion detection system based on learning program behavior. In: Debar H, Mé L, Wu SF, edtiors. Recent Advances in Intrusion Detection. RAID 2000. Lecture Notes in Computer Science, Volume 1907. Berlin, Germany: Springer; 2000. pp. 93–109.
4. Shitharth S, Prasad KM, Sangeetha K, Kshirsagar PR, Babu TS, Alhelou HH. An enriched RPCO BCNN mechanisms for attack detection and classification in SCADA systems. IEEE Access. 2021; 9: 156297–156312.
5. Akojwar S, Kshirsagar PR. A novel probabilistic-PSO based learning algorithm for optimization of neural networks for benchmark problems. WSEAS Trans Electron. 2016; 7: 79–84.
6. Albishry N, AlGhamdi R, Almalawi A, Khan AI, Kshirsagar PR BaruDebtera. An attribute extraction for automated malware attack classification and detection using soft computing techniques. Comput Intell Neurosci. 2022; 2022: Article 5061059.
7. Jude AB, Singh D, Islam S, Jameel M. An artificial intelligence based predictive approach for smart waste management. Wireless Pers Commun. 2021; 127 (1): 1–21.
8. Chandan RR, Kshirsagar PR, Manoharan H, El-Hady KM, Islam S, Khan MS, Chaturvedi A. Substantial phase exploration for intuiting Covid using form expedient with variance sensor. Int J Computers Commun Control. 2022; 17 (3): Article 4539.

