IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-12, Dec 2018 E-ISSN: 2347-2693

Impact of Artificial Intelligence on Cyber Security

Rashmi B H

Department of Computer Science & Engineering, Global Academy of Technology, Bangalore, India

Corresponding Author: rashmihariharan94@gmail.com

Available online at: www.ijcseonline.org

Accepted: 16/Dec/2018, Published: 31/Dec/2018

Abstract: As the technology is evolving day by day, new challenges are coming in a computing world. One such challenge is Cyber Security. Cyber Security is also termed as Computer security or Information Security. Cyber security experts are facing lot of problems with the outburst of technologies like IOT. In order to avoid these outbursts Cyber security experts should be aware of many security attacks and breaches and should be in a position to classify all the attacks and prevent the system from these types of attacks. But due to heavy traffic and many more security breaches, the areas under Cyber security threat can't be handled by humans. It is quite difficult to create standard automation algorithms to prevent certain Cyber area threats. To implement these standard automation algorithms, an area of Intelligence called as Artificial Intelligence is adapted. Using these Intelligence techniques many security breaches and cyber-attacks can be avoided. This paper focuses on Artificial Intelligence applications and techniques for Cyber Security, in order to be responsive to many Cyber-attacks.

Keywords: Cyber Security, Artificial Intelligence, CAPTCHA, Expert Systems, Neural nets, Intelligent Agents.

I. INTRODUCTION

With the advent changes in technologies, maintaining security in and around Cyber area is an open challenge. In order to prevent certain Cyber threats integration of Artificial Intelligence with Cyber Security has been taken up as a global business challenge to prevent certain network security attacks and breaches. In olden times Information or Computer security and Artificial Intelligence was treated as 2 separate entities in maintaining security , but with the increase of many attacks and security breaches, humans alone could not monitor heavy traffic causing in Cyber area. To overcome this certain standard algorithms involving Artificial Intelligence is evolved to main the Integrity and Confidentiality of the data. One best example of this integration of AI with Cyber security are CAPTCHAs, which is one of the pattern recognition techniques wherein the client side will be the Symbols or Pictures or Letters and server side will be for the user to identify the pictures based on the questionnaire or to type the letters or symbols in order to pass the authentication and authorization credentials. This particular example proves to be an immense step towards Artificial Intelligence (AI) innovation. Artificial Intelligence is having immense demand in modern day technologies, as it has many applications in the areas like Healthcare by solving many issues related to Medical dosages, in the advancements of Automotive industries by developing new automation technologies like driverless cars, in the field of

Finance and economics to detect fraud and claims in global businesses and also Artificial Intelligence has wide applications in the areas like Video gaming, Military, advertising and many more. Likewise Artificial Intelligence is being integrated with Cyber security to provide security in cyber area by providing many techniques like

- Expert Systems
- Neural Network
- Intelligent agents
- Search & Learning

Figure 1: AI in Cyber Security

Section II explains different techniques of AI involved in securing Cyber threat areas. Section III explains Artificial Intelligence and Cyber security applications. Section IV portrays Artificial Intelligence challenges and Section V consists of Conclusion and Future scope.

II. TECHNIQUES OF AI

The following are the techniques of Artificial Intelligence integrated with Cyber Security to prevent certain security attacks and breaches. They are as follows:

- **EXPERT SYSTEMS**

Expert system is an Artificial intelligence tool which enhances the decision making ability of humans under Cyber area. Basically these tools of AI are developed to solve complex problems. Expert systems were the first successful tool of Artificial Intelligence. Expert systems are divided into 2 subsystems as shown in the Figure 2. The inference engine and Knowledge base. Inference engine does the task of applying rules to known facts to bring in new rules, whereas Knowledge base has certain applications like debugging capabilities.

Advantages of Expert Systems

- Rules were specified and reviewed in a precise way so that it was easily understood.
- Knowledge base helped in rapid development of new technologies.
- Ease of maintenance.
- Implemented Rapid Prototyping.

Disadvantages of Expert Systems

- Suffers from Knowledge acquisition problem
- With the usage of old tools of Expert system, performance decreased drastically.
- System and database integration was complex.

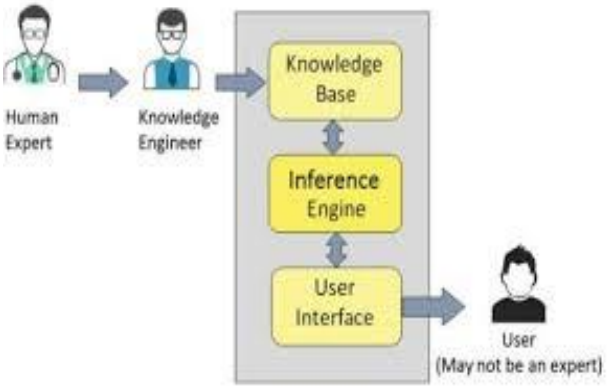

Figure 2: Expert System in AI

- **NEURAL NETWORK**

Neural network is the advanced branch of AI, which is also called as Deep Learning. It works similarly as the functioning of Human Brain. Basically these neural networks are domain-independent and can learn about various types of data. Similarly when this concept is applied in Cyber Security, the system acts as domain-independent and can easily identify whether a stored file is malicious or legitimate without human interaction. So this technique of Artificial Intelligence when combined with Cyber Security prevent malicious agents entering into the network and also illegitimate access to network. Neural nets differentiates the documents based on malicious property or legitimate depending on human intervention. The main advantage of using Neural nets is that it prevents certain malicious agents entering into the Cyber area and prevents organization from certain attacks.

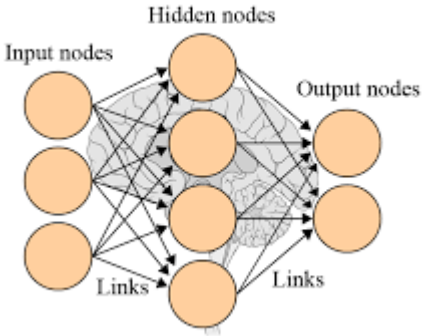

Figure 3: Neural Network in AI

- **INTELLIGENT AGENTS**

In Artificial intelligence, Intelligent agent acts as an entity which combines sensors and actuators to model the system and function as a Computer program. Intelligent agents in AI project themselves as Abstract Function agents. Hence intelligent agents in AI is also called as Abstract Intelligent Agents (AIA). The most common example of intelligent agents is Thermostat. The main advantage of using Intelligent Agents in Artificial agents is that these agents acts as a Protection against Distributed Denial of Service (DDoS) attacks. These Intelligent agents should develop a "Digital Police" or "Cyber Police", to have an eye on Business documents having legitimate access. So these developed products should consist of very active intelligent agents. To carry out this process, a well-planned Infrastructure to be developed in order to maintain the quality and to have a close Interaction with intelligent agents. Therefore these Intelligent agents are Proactive and reactive in nature and provides protection against various DoS attacks.

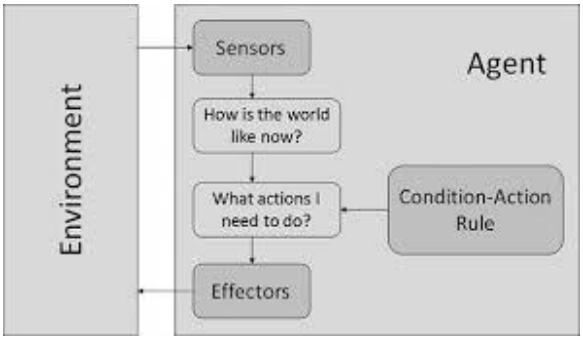

Figure 4: Intelligent Agents in AI

Artificial Intelligent techniques are ideal for preventing Cyber security attacks by considering 2 main points namely:

- AI techniques can take an advantage of good software's, prepare them and update the rules and use them to improve security.

- Large amount of good data is present and can be utilized effectively for security purpose.

III. ARTIFICIAL INTELLIGENCE & CYBER SECURTY APPLICATIONS

CYBER ATTACKS: The main aim of maintaining Security in Cyber environment is to protect the system from Hackers and also Software errors and Failures. There is a need for the development of the system that can detect and correct errors and also to defend against many types of incoming Network attacks. So integrating Artificial intelligence techniques in Cyber Security could lead to the development of such systems which could search and repair errors before they enter in to the Cyber area.

Figure 5: Hackers & Cyber Attack

CRIME PREVENTION: An early form of Artificial Intelligence called Computer Statistics was used to prevent certain cyber-crimes in Cyber environment. It is using a tool called Predictive Policing, where in artificial intelligence is combined with game theory to prevent Cyber-crime under Cyber area.

Figure 6: Cyber-crime and AI

PRIVACY PROTECTION: Privacy is one of the major concern of issue in today's complex world. Certain automation algorithms involving Artificial Intelligence have been used to improve privacy in and around us.

Figure 7: Privacy Protection with AI

IV. CHALLENGES

Artificial Intelligence is becoming a ray of hope in the field of science and technology. Some of challenges to be considered for an Effective AI system.

- An Artificial Intelligence system should not have any negative effects while performing the task.
- The given AI system should have a scalable oversight.
- As more research goes into new technologies like machine learning, deep learning, AI is becoming smarter and self-developing by replacing humans.

V. CONCLUSION & FUTURE SCOPE

In the present scenario, we can see a rapid increase in Cyber threats. To prevent this an effective intelligent security system is needed. In order to have an effective intelligent system, Artificial intelligence techniques are considered because these are more robust than Cyber security solutions. Therefore AI has a great impact on Cyber Security and its related frameworks. Artificial Intelligence can be used in various ways for the benefit of Cyber Security. As a Future scope still more efficient intelligent systems should be developed in order to make our Cyber environment more safe and secure.

REFERENCES

[1] Arockia panimalar, Giri Pai,"*AI Techniques for Cyber Security*", IJRET, Volume: 05, 122-124.
[2] Arpitha, kaustubh Dutta, "*Impact of Machine Learning and Artificial Intelligence on Mankind"*,I2C2,2017.
[3] Narendra kumar, Nidhi, Rashi," *Ethical aspects and Future of AI*",2016,ICICCS,111-114.
[4] Arlindo Oliveria," *Cyber Security and role of Artificial Intelligence*".
[5] Dr. Sunil Bhutada, Preethi Butada," *Applications of AI in CyberSecurity*",IJERCSE,Volume 5,Issue 4,214-219.
[6] P. Santra*,"An Expert Forensic Investigation System for Detecting Malicious Attacks and Identifying Attackers in Cloud Environment"* Research Paper | Journal (IJSRNSC) Vol.6, Issue.5, pp.1-26, Oct-2018

Author Profile

Rashmi B H pursued Bachelor of Engineering from Global Academy of Technology, Bangalore in 2015 and secured 3rd rank for the University and Master of Technology from BNM Institute of Technology in the year 2017 and is a first rank holder and a Gold medalist from VTU University. She is currently working as Assistant Professor in Department of Computer Science & Engineering, Global Academy of Technology since Jan 2018.She has published many research papers in reputed and UGC approved Journals. Her main research area interests is on Network security, Cyber Security, Artificial Intelligence, Cryptography and Computer networks.

