How Artificial Intelligence Works in Cyber Security

Sharvaree Joshi
Student
Department of Master of Computer Application
IMCOST College, India

Abstract— As technology is evolving day by day, new challenges are coming out. Dealing with the increasing data, connected devices the data security has become a challenge. The cybersecurity expert faces various problems with the advancement in technology. In order to maintain cyber security, experts should be aware of various attacks with latest trends, security breaches to identify the threats. Due to heavy network traffic, intrusions the areas under cybersecurity assaults cannot be handled by only humans. For these threats, the cyber expert needs the full proof resolution in AI. With the advantage of AI, threats and intrusions can be easily detected without the involvement of humans. To implement standard automation algorithms, the AI is adapted for cybersecurity. This paper focuses on how AI algorithms work in identifying cyber threats and find out with an appropriate resolution.

Keywords: Artificial Intelligence, Cyber Security, Expert System Neural Networks, Intelligent Agent

I. INTRODUCTION

With the advancements in technology and digitization, dealing with a humongous data, connected gadgets and devices has now become a manageable task. However, maintaining the cyber security in any organization has remained an open challenge. In order to prevent the cyber threats, various attacks and also to refrain organizations from network intruders and any possible security breaches, the network scientists are hunting for full proof resolution in Artificial Intelligence. As one can see, multiple business networks lead to heavy network traffic and generate vast amount of data and information that cannot be handled only by human but with the support of technology. In older times the Cyber security and artificial intelligence considered as the two separate entities. However, with the advantage of Artificial Intelligence, automation in detecting threats without involvement of humans has become possible. Artificial intelligence is completely machine language driven system which assure us error-free cyber security services. Cyber security computes the application and analyses the views of improving the cyber security techniques by acquiring AI algorithms and existing techniques.

A. Purpose and need of AI in Cyber Security:

Artificial Intelligence researchers were interested in developing the programs to reduce the human work while cyber experts are trying to improve the cyber security with the overflow of information. As the technology evolves, Artificial intelligence and cyber security gets closer to solve the cyber issues, not only at human user level but also at the lower system framework. Progress in machine learning techniques means that AI application can also adopt the changes in the cyber threats and deduct the problems that arises.

The purpose of this paper is to describe AI techniques in cybersecurity. Nowadays organizations used to store the data digitally. With the advancement in digitalization, data security has remained an open challenge. To prevent the various cyber-attacks, the system itself should be able to handle the cyber threats without human interaction. AI has a number of algorithms which can be used for preventing such attacks. With the help of AI, a cyber expert can easily identify the network intrusion, data theft, denial of services, malicious activities.

B. Definitions and techniques of Cyber security and AI:

Artificial intelligence (AI), the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.

Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

1) AI Techniques in cyber security:

Following are the techniques of AI integrated cyber security attacks and threats:

a) Expert System:

An Expert System that replicates the "decision making" abilities of humans under cyber area. Basically this technique is used to solve the complex problems. It is also used for arranging security in cyber defence. Expert System was the first tool of AI which is categorised into 2 parts.

– Knowledge base expert system:

The Knowledge base system comprises the knowledge which is stored regarding a particular domain. It also incorporates the interface engine for the inferring knowledge of present system as well as the further knowledge of particular circumstances.

Components:

– Malicious IP Address
– Known Malware
– Known Virus
– Approved applications
– Interface engine expert system:

Interface engine is a component of the system that applies the logical rules to the knowledge base system to deduce the new information. Interface engine is automated reasoning system.

Components:

– IP Address Geographical Location
– Connection attempts
– Connection Patterns

- Document Usage
- Login Timestamps
- Login Attempts

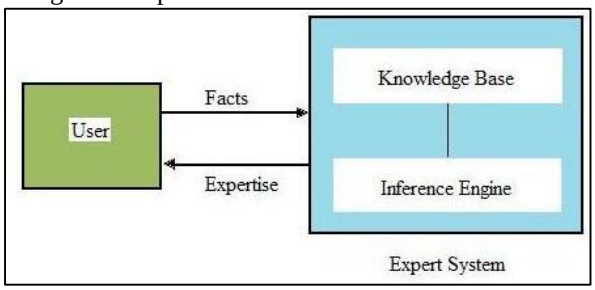

Fig. 1: Expert system in AI

b) Neural Network:

Neural networks are the advanced techniques in the AI, which is also known as deep learning. It works similarly as the functioning of the human brain. Our brain has several neurons, which are domain-independent. Similarly when this concept applied to cyber security, the system acts as domain-independent and can easily identified whether the file is malicious or legitimate. So this technique of advanced AI can be used in cyber security for detecting network intruders and illegal access into the network. The main advantage of this technique of AI in cyber security is to prevent the illegal access into the network and malicious activities in the system and prevent the system from this cyber-attacks.

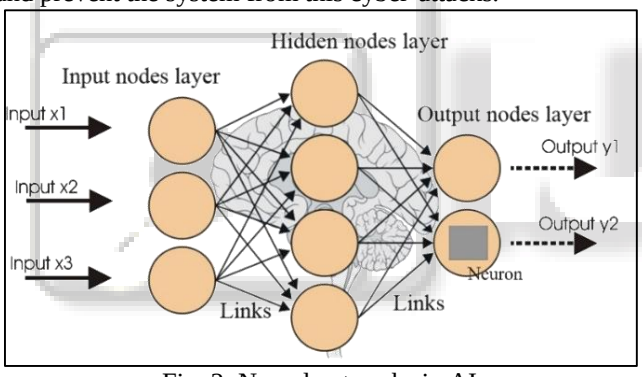

Fig. 2: Neural networks in AI

c) Intelligent Agent:

Intelligent agents are the self-sufficient computer system, which communicate with each other to share the information in order to actualize the proper reaction. In Artificial intelligence, intelligent agent acts as an entity which combines sensors and actuators to model the system and function as a Computer program. The mobility and adoptability of the intelligent agent, makes them competent to fight any unforeseeable condition. Intelligent agent in AI project themselves Abstract Intelligent Function. The main advantage of intelligent agent is that is protection against Distributed Denial of Services (DDoS) attacks. In case if there is any legal or business issue, it should be manageable to develop a "Cyber Police". Cyber Police should have mobile intelligent agents. For this we should device the infrastructure to support the quality and interaction between the intelligent agents. Multi-agent tools will give a lot of operative appearance of the cyber police.

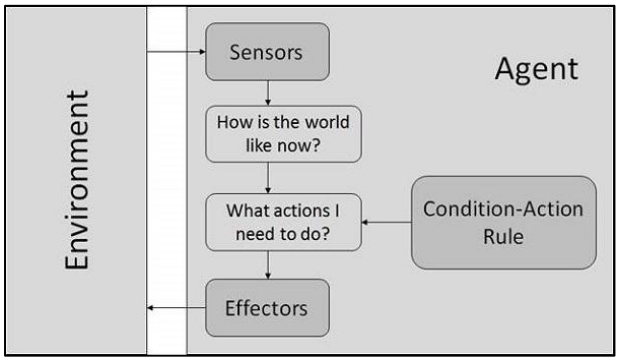

Fig. 3: Intelligent agent in AI

C. Current Strategies of Cyber Security and AI:

In the current scenario, all the companies face some kind of cyber-attacks even if the strong precautionary measures have already been taken. 76% of India businesses were hit by the cyber-attacks in 2018 as per the survey (by UK-based endpoint security provider Sophos). The survey also says that India was the country with third highest number of cyber-attacks in 2018, according to the report, after Mexico and France. Using AI, can be very helpful in dealing with the data security of any organization. A good cyber security strategy identifies the malicious activities in the network as well as recognizes the patterns in the search criteria, and also categorizes the spam emails and other aspects of the security. Here are some of the big companies that have adopted the AI.

1) Google:

Gmail has used machine learning techniques to filter the emails since its launch 18 years ago. Today, we have the Google Assistant which is released in May, 2018. It helps to recognize the voice commands and communicates with user by the natural voice and accent.

2) IBM/Watson:

The team IBM has increasingly leaned on its Watson Cognitive learning platforms for "Knowledge consolidation" tasks and threat recognition based on machine learning.

3) Balbix:

Breach Control platform uses AI-powered observations and analysis, to deliver continuous risk predictions, risk based vulnerability management and proactive control of breaches.

D. Statement of Problem

How Artificial Intelligence can be used to control Cyber security breach.

E. Objective

- To study the techniques and algorithms of AI in cyber security.
- To study the effectiveness of AI technology in cyber security of the organization.

F. Hypothesis:

If developed a suitable AI, it can be used as an effective tool for Cyber Security.

G. Limitations:

- Trying to use a range of AI tools can be expensive and time consuming
- AI may require regular upgrades to adapt to continually changing business environment

II. DESIGN OF STUDY

A. Introduction:

As indicated in the primary chapter, the purpose of this research paper was to find the effectiveness of AI in cybersecurity.
This section includes:

B. Research Methodology:

In general, the research design is like a blueprint for the research. It provides insights about "how" to conduct research using a particular methodology.

In this research, the explanatory research method is used. Explanatory research focuses on explaining the aspect of study in a detailed manner. The Explanatory research is not used to give us some conclusive evidence but helps us in understanding the problem more efficiently. Explanatory Research is conducted for a problem which was not well researched before, demands priorities, generates operational definitions and provides a better-researched model.

C. Explanatory Research design:

1) Increasing Understanding:

Nowadays there are various cyber-attacks like data theft, malware, denial of services and many more take place in the organizations. In the small and middle scale organizations there is a lack of technical resources to protect the data from cyber-attacks. Due to the lack of security, cyber-criminals generally target the small and medium scale businesses.

2) Better Conclusion:

Using the AI in cybersecurity can be useful to prevent or identify cyber-attacks take place in the system. AI consists of the number of algorithms which we can apply to cyber threats and find out a better way to overcome the data loss.

III. CONDUCT OF STUDY

A. Introduction:

This research paper aimed at the effective use of AI techniques in cybersecurity. This section includes the comparative study of AI algorithms and tries to find the better one which can implement in cybersecurity.

B. Comparative Study of AI Algorithms:

1) Expert System:

In general, an expert system is a knowledge-based system that employs knowledge about its domain and uses in an interfering procedure to solve problems. It generally helps to solve the complex problems in a specific domain. It has a level of human intelligence and expertise. Application areas of the expert system include classification, diagnosis, monitoring, process control, design, scheduling and planning, and generation of options. An expert system is composed of two major components, the Knowledge-based system, and Interface engine.

Knowledge-based of an expert system is a store of both factual and heuristic knowledge. Factual knowledge is the information widely accepted by the Knowledge Engineers in the task domain. Heuristic Knowledge is about practice, accurate judgment, one's ability of evaluation, and guessing. The representation of these algorithms is the method used to organize and formalize knowledge in the knowledge-based system. It is in the form of IF-ELSE-THEN rules. The success of any expert system majorly depends on the quality, completeness, and accuracy of the information stored in knowledge-based.

Interface Engine is a component of the system that applies logical rules to the knowledge-based system to deduce the new information. The interface engines work primarily one of two modes: forward chaining or backward chaining. Forward chaining starts with the known facts and asserts new facts. Backward chaining starts with goals and works backward to determine what facts to be asserted.

a) Advantages of Expert System:

- Consistency: An expert system is computer-based, all the logic or knowledge programmed into it. If the same situation occurs again and again, it will make the same decision again and again.
- Intrusion detection: Due to high performance, an expert system can easily identify any malicious activity or intrusion detection with the help of prerequisite knowledge.
- Memory: It has a huge amount of memory to store a large amount of knowledge with equal accessibility.
- Logic: In an expert system, all the rules and conditions are programmed to making a decision more efficiently.

b) Disadvantages of Expert system:

An expert system is not a complete solution to any problem.

- Time and cost: The time and cost required to buy an expert system are very high. It requires a huge amount of time to acquire a knowledge which is needed to develop an expert system.
- Specific: The expert system is generally developed for the specific domain.
- Common-sense: The expert system can take the right decision as they are programmed with some rules and regulation. So they can't provide a completely new solution to any problem.

2) Neural Networks:

Neural networks are a set of algorithms that are designed to recognize the patterns. The patterns they recognized are numerical, contained in vectors, into which all real-world data, be it images, sounds, text, or time series must be translated. Neural networks generally use clusters or classifications. They help to group unlabelled data according to similarities among example inputs.

a) Classification:

All the task are classified which depends upon labelled dataset. Human must transfer their knowledge into a dataset to study the correlation between the labels and data. This is known as supervised learning. Supervised learning provides algorithms with known quantities to support future learning.

b) Clustering:

Clustering is the detection of similarities. It does not require any label to detect similarities. Learning without labels is known as unsupervised learning. In unsupervised learning, an AI system may group a piece of unsorted information even if there are no categories provided.

c) Regression:

Regression estimates a continuous dependent variable or response from a list of input variables. The regression is a predictive analysis of the data inputs. Regression uses the

historical relationships between an independent and dependent variable to predict future output. Businesses use regression to predict such things as future sales, stock prices, currency exchange rates, from training programs.

When we apply neural networks algorithms to cybersecurity, the system can identify whether a file is malicious or legitimate without human interference. This technique yields a strong result in detecting malicious threats, compared with classical machine learning systems. Neural networks are helpful to find out the intrusion detection as well as intrusion prevention.

d) Advantages of neural network:

- Ability to solve complex problems: Neural network has the ability to learn non-linear or complex relationships as it works like a human brain.
- A neural network can generalize: After learning from initial input, it can infer unseen relationships on unseen data, thus making model predict on unseen data.
- DoS detection: In the case of cybersecurity it helps to find the denial of service attacks in the system. It is also used in the foreign investigation to identify threats.

e) Disadvantages of Neural network:

- Hardware dependence: It require processors with parallel processing power with their structure.
- Determination of proper network structure: there is no any rule for determining the structure of neural network in AI.

3) Intelligent Agent:

In an Artificial Intelligent, an intelligent agent acts as an entity which combines sensors and actuators to function like a computer program. An AI agent can have mental properties such as knowledge, belief, and intention.

a) Sensor:

It is a device which detects the change in the environment and sends the information to other electronic devices.

b) Actuators:

These are the components that convert energy into motion. This is responsible for monitoring and controlling the system.

c) Effectors:

These are the devices of the system which affects the environment.

d) Rational agent:

These are agents which have clear preference, models uncertainty and acts in a way to maximize its performance. Rational agents are used for game theory and decision theory for real-world scenarios. The rationality of these agents is measured by their performance. Following are the key points which help to measure the performance:

- The performance measures the degree of success.
- Prior knowledge of its environment.
- Best possible actions to perform.
- Percept sequence till now.

In cybersecurity, the main advantage of using Intelligent Agents in Artificial agents is that these agents act as a Protection against Distributed Denial of Service (DDoS) attacks. It has behaviour like understanding agent interaction language, pro-activeness, and reactivity. They can adapt to real-time, learn new things rapidly through communication with the environment, and have memory based standard storage and recovery abilities.

e) Advantages of Intelligent agent:

- Mobility: Intelligent agents engaged across the different system architecture and platforms and gather various information.
- Goal oriented: It has the ability to accept the user statement of goal and carry out the task.
- Independent: It functions on its own without human interference. So it has the ability to make decisions without human supervision.
- Reduces network traffic: Agents can communicate with each other quickly. It enables them to search task quickly and more efficiently and reduces network traffic.

f) Disadvantages of intelligent agent:

- No overall system controller: Intelligent agents are not fully independent. Sometimes it may not be appropriate where there are global constraints that need to be enforced.
- No global perspective: It can only make decisions based on locally accumulated knowledge.
- Trusting delegation: As a user is giving the responsibility of data acquisition and decision making, so for the security purpose, they must sure that they can trust the system.

C. Recommendation:

While doing the comparative study of the algorithms of AI, in case of cyber-security we can apply any of the algorithms for various types of cyber-attacks. These techniques are more flexible than contemporary cybersecurity solutions. There is a need to develop the system like AI which can detect and prevent the cyber-attacks and also find the network intrusion and detection.

Neural network algorithms are more efficient for the detection and prevention of the cyber-attacks. Malware detection and network intrusion detection are the major areas where the neural network algorithms can show significant improvements over the classic machine learning problems. Using a neural network of AI in cybersecurity can play an important role in achieving the highest rates of detections in industry and also provide prevention through independent tests.

Before applying the techniques of neural networks, we should consider the following:

- Time and cost-effectiveness of resources
- Upgradation of required software
- Number of resources
- Memory

IV. CONCLUSION

From this study, it could be concluded that, in order to efficient intelligence, Artificial intelligence techniques are more robust than contemporary cybersecurity solutions. Though we have seen a number of algorithms for various cyber-attacks, then artificial intelligence may be a solution for the future cyber-attacks. When a human opponent with a clear by-passing goal attacks the intelligent security the system may fail. This doesn't mean we should not use Artificial Intelligence techniques, but we should know its limits. An Artificial Intelligence technique needs continuous human communication and training.

V. SUGGESTION FOR FURTHER STUDY

Future research could be applying AI techniques in the industry for cyber-attacks detection and prevention. The study will be also conducted the future of AI in cyber prevention and actual implementation of AI. While doing so, the techniques selected are not so much complicated at a technical level.

REFERENCES

[1] 76% Indian businesses hit by cyber-attacks in 2018, finds survey - Devika Singh, New Delhi, Last Updated: March 13, 2019 | 19:04 IST https://www.businesstoday.in/current/economy-politics/76-per-cent-indian-businesses-hit-by-cyber-attacks-in-2018-finds-survey/story/327389.html
[2] ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY, Arockia Panimalar, Giri Pai, Salman Khan. Volume 05, Issue 03, Mar-2018. https://www.irjet.net/archives/V5/i3/IRJET-V5I327.pdf
[3] Impact of Artificial Intelligence on Cyber Security, Rashmi B H, Vol.-6, Issue-12, Dec 2018. https://www.ijcseonline.org/pub_paper/56-IJCSE-05414.pdf
[4] NEURAL NETWORKS IN CYBER SECURITY, J.Rubina Parveen, Issue 09, Volume 4 (September 2017). http://www.irjcs.com/volumes/vol4/iss09/08.SISPCS10095.pdf
[5] Artificial Intelligence in Cyber Defense, Enn Tyugu, 2011. https://ccdcoe.org/uploads/2018/10/ArtificialIntelligenceInCyberDefense-Tyugu.pdf
[6] Five current limitations of Artificial Intelligence to marketers, by Emma mullan , 20 December 2018. https://blog.hurree.co/blog/limitations-of-artificial-intelligence-mobile-marketing
[7] Using power of deep learning for cyber security (Part 1), Guest blog, July 5, 2018. https://www.analyticsvidhya.com/blog/2018/07/using-power-deep-learning-cyber-security/

