EasyChair Preprint

№ 5791

Artificial Intelligence (A.I.) and It's Application in Cyber Security

Suyash Srivastava and Bejoy Benny

June 15, 2021

ARTIFICIAL INTELLIGENCE (A.I.) AND IT'S APPLICATION IN CYBER SECURITY

Suyash Srivastava[1], Bejoy Benny[2]

Mentor Priyanka Grover Ma'am, Neha Batra Ma'am

[1]Department of Computer Science Engineering (Cyber Security Forensics), Manav Rachna International University, Faridabad, India

[2]Department of Computer Science Engineering (Cyber Security Forensics), Manav Rachna International University, Faridabad, India

ABSTRACT

One of the major issues we face in this rapidly advancing world is the evolution of threats that occur with the evolution in science. Cyber security is one of the main concerns that technical world has to deal with in this digital civilization. Number of cyber threats and cyber-crimes are taking place even as we are reading this paper right now. Cybercrimes including cracking of cryptography data, hacking of servers, Data breaches, ID thefts and many more challenges [2]. With the advancements in the field of Artificial intelligence and ML these risks are shooting high in numbers with an exponential curve. A.I. has made its way into almost every field be it in healthcare for detecting cancers using data or using facial recognition systems for logging into devices as well as websites. These risks affect a large number of individuals and companies as well. That is why there is a need to learn the use of A.I. in cyber security to avoid the attacks that can be "intelligently" executed and exploit the vulnerabilities [1]. In this report we will discuss about some future scopes of A.I. and its efficient use in Cyber Security fields.

KEYWORDS

Artificial intelligence, Cyber security, Cyber-crimes, Intelligent Cyber Security techniques, Artificial intelligence in Cyber Security, Applications of Artificial Intelligence.

1. INTRODUCTION

Artificial Intelligence, a type of “Intelligence” that is man-made to stimulate processes that are human-alike or to reduce repeated labor. Humans can be distinguished from anything present in this world by the measure of this specific term “Intellect”. Cybersecurity is important because it encompasses everything that pertains to protecting our sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems from theft and damage attempted by criminals and adversaries.

A.I. and Cyber security both are the fields of technology that when combined together might form a boon for the future and might risk as bane for the future as well. To execute a persistent and versatile protection, Cyber security systems must adapt to the changing environment as well by conforming to changes and threats involved in digital game. The new security ways like dynamic setup of secured perimeters, comprehensive scenario awareness, extremely machine-driven reaction on attacks in networks would require wide usage of AI ways and knowledge-based tools [4]. With all this technology we can hope to keep the database of employees and users safe much efficiently from cyber-attacks that are happening occasionally. This clears the basic motive of this research paper which is to discuss that with revolutionizing technology in Machine learning and A.I., there is a need to protect huge amounts of data sets and database that could be carved down in fraction of seconds, with the role of A.I. in Cyber security we may be able to identify these security threats and take measures accordingly [3].

1. PROBLEM STATEMENT

Internet has now evolved and it’s usage is spread so vastly that it even comes in the “essentials” of survival in the daily routine of modern generation. With millions of billions of data packets and information being shared and exchanged online, the risks of exposure of same data has become a huge problem now [5]. The vulnerability of users and threats caused by increased number of cyber-attacks increase at a dramatic rate. Therefore, we need to find a way to overcome this problem by continuous adaptation of security systems even as we speak. Thus, we need to discuss about the various applications A.I. and how it prevents cyber-attacks by helping in cyber security techniques [7].

2. A.I. TECHNIQUES IN CYBER SECURITY

We already know that as we move forward, we will be encountering even greater technologies and machines that will be smarter. As the technology is evolving and getting complex with time, similarly the threats and assaults they need to deal with are enhancing and getting smarter [7]. To counter these attacks and keep the data safe and unexposed, we need the following A.I. techniques in our cyber security systems.

Table 3.1. AI techniques and their usage

AI Techniques	Usage
Application of Intelligent Agent	• Proactive • Agent communication language • Reactive • Defense 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)

The above table shows the advantages and techniques summarised in a table. Let’s discuss about these techniques and how exactly are these beneficial for protection against cyber-crimes in detail.

2.1 INTELLIGENT AGENTS

Intelligent agents are self-sufficient computer system created force that communicate with each other to share information and participate to each other so as to arrange and actualize proper reactions if there should arise an occurrence of unforeseen occasions [8]. Their mobility and adaptability in the conditions they are conveyed in, and in addition their synergistic nature, intelligent agent technology appropriate for fighting cyber assaults.

These intelligent systems are very useful in protecting against DDoS (Distributed Denial of Service) assaults. Infrastructure must be installed as for the movement and communication supports the cyber agents [9]. For entirely efficient and operational picture of a Cyber space, we need a Multi-agent Tool, for example, a neural network-based intrusion detection and hybrid multi-agent techniques. Intelligent agents are often described schematically as an abstract functional system similar to a computer program. Researchers such as Russell & Norvig (2003) consider goal-directed behaviour to be the essence of intelligence; a normative agent can be labelled with a term borrowed from economics, "rational agent". In this rational-action paradigm, an IA possesses an internal "model" of its environment. This model encapsulates all the agent's beliefs about the world.

The agent also has an "objective function" that encapsulates all the IA's goals. Such an agent is designed to create and execute whatever plan will, upon completion, maximize the expected value of the objective function. A reinforcement learning agent can have a "reward function" that allows the programmers to shape the IA's desired behaviour, and an evolutionary algorithm's behaviour is shaped by a "fitness function". Abstract descriptions of intelligent agents are sometimes called abstract intelligent agents (AIA) to distinguish them from their real-world implementations as computer systems, biological systems, or organizations. Some autonomous intelligent agents are designed to function in the absence of human intervention. As intelligent agents become more popular, there are increasing legal risks involved [15].

2.2 EXPERT SYSTEMS

An expert system is a computer program that uses artificial intelligence (AI) technologies to simulate the judgment and behaviour of a human or an organization that has expert knowledge and experience in a particular field. Typically, an expert system incorporates a knowledge base containing accumulated experience and an inference or rules engine -- a set of rules for applying the knowledge base to each particular situation that is described to the program. The system's capabilities can be enhanced with additions to the knowledge base or to the set of rules [5]. Current systems may include machine learning capabilities that allow them to improve their performance based on experience, just as humans do. The concept of expert systems was first developed in the 1970s by Edward Feigenbaum, professor and founder of the Knowledge Systems Laboratory at Stanford University. Feigenbaum explained that the world was moving from data processing to "knowledge processing," a transition which was being enabled by new processor technology and computer architectures.

Expert systems have played a large role in many industries including in financial services, telecommunications, healthcare, customer service, transportation, video games, manufacturing, aviation and written communication. Two early expert systems broke ground in the healthcare space for medical diagnoses: Dendral, which helped chemists identify organic molecules, and MYCIN, which helped to identify bacteria such as bacteraemia and meningitis, and to recommend antibiotics and dosages. A more recently developed expert system, ROSS, is an artificially-intelligent attorney based on IBM's Watson cognitive computing system. ROSS relies on self-learning systems that use data mining, pattern recognition, deep learning and natural language processing to mimic the way the human brain works. Expert systems and AI systems have evolved so far that they have spurred debate about the fate of humanity in the face of such intelligence, with authors such as Nick Bostrom, professor of philosophy at Oxford University, pondering if computing power has surpassed our ability to control it.

The Security expert system follows a set of rules to battle cyber-attacks. It checks the process with the knowledge base if it is good known processes then the security system ignores otherwise the system would terminate the process. If there is no such process in knowledge base, then using inference engine algorithms (rule sets), the expert system finds out the machine state. The machine state has been composed into three states namely safe, moderate and severe. According to the machine state, the system alerts the administrator or the user about the status,

and then the inference has been feed to Knowledge base. FRBCES (Fuzzy Rule Based Cyber Expert System) is one of the rule based expert system for cyber-attacks [4].

2.3 VISUAL NETS/ NEURAL NETS

Visual nets, better known as neural nets start from way back in 1958 when Frank Rosenblatt came up with the invention of a perceptron – a man-made nerve cell that has remained one among the foremost well-liked components of neural nets.

Already a little variety of perceptron's combined along will learn and solve fascinating issues. However, the neural nets will include a wider range or variety of artificial neurons. So neural nets offer a practicality of massively parallel learning and decision-making [13]. Their most distinguished feature is that the speed of operation. They're well matched for learning pattern recognition, for classification, for choice of responses to attacks etc. they will be enforced either in hardware before in software system. Neural nets are well relevant in intrusion detection and intrusion bar [11].

There are proposals to use them in DoS detection, pc worm detection, spam detection, zombie detection, and malware classification and in rhetorical investigations. One of the major reasons for the recognition of neural nets in cyber security is their quickness or fast speed, if enforced in hardware or utilized in graphic processors [9].

There are new developments within the neural net's technology: third generation neural nets prickling neural networks that imitate organic neurons a lot of realistically, and supply a lot of application opportunities [12]. Neural networks in face recognition system plays an important role in AI for cyber-security [14].

2.4 MACHINE LEARNING

In the world of Machine learning, the most basic approach involves computational strategies for procuring new knowledge, and also use previous knowledge data to reach new heights [16].

The learning problem varies depending upon parametric complexity, from simple parameters to symbolic ones decide the complicating factor, for example, the method of concept learning, even recognizing behavioural patterns, the grammar as well as the functions. Both supervised learnings and unsupervised learning techniques can be used to achieve this [6].

Usually for larger data sets or large amount of data instead of using supervised learning we take unsupervised learning into consideration. For example, Cyber defence techniques make use of expansive logs by using unsupervised learning. The concept of Data Mining that is being in a wide use nowadays was initially derived from the unsupervised learning. Also a useful of neural nets are used in unsupervised learning, specifically in Self Organizing Maps [17].

Parallel learning algorithms that are executed on the parallel hardware platforms also fall under these learning methods. To present the same, we use Genetic algorithms as well as Neural nets to represent the learning methods.

3. DATA ANALYZATION OF CYBER ASSAULTS

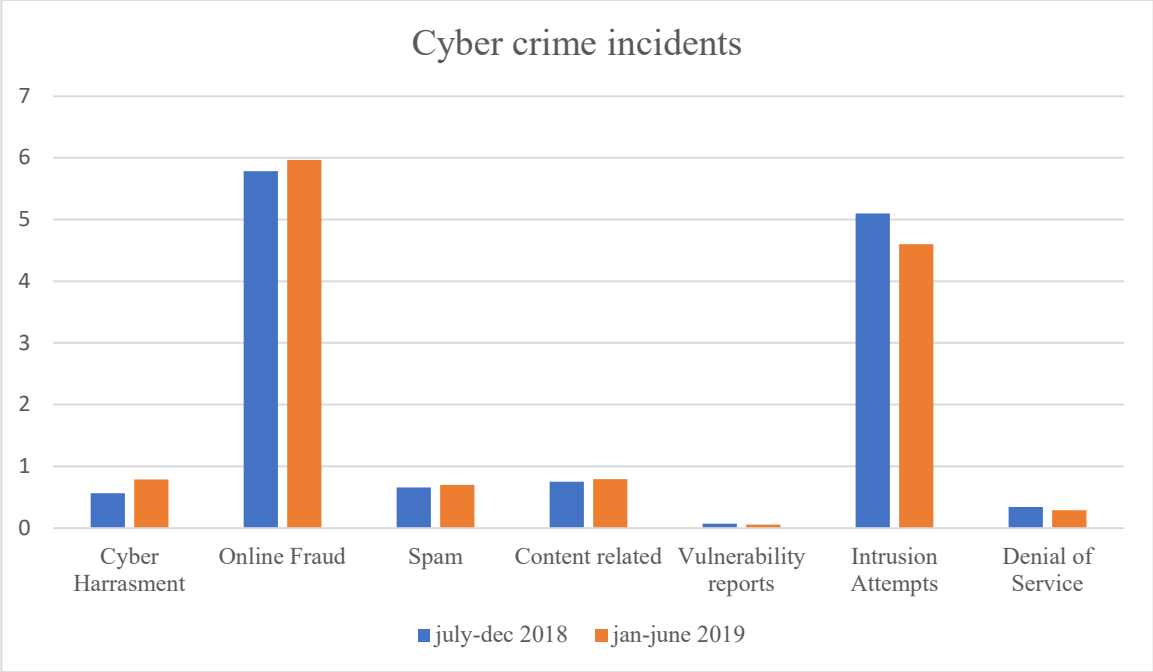
The following information and data are collected from a secondary source. The data will talk about the analysis and the rate of cyber-crime status in India which was witnessed during the year 2018-19.

Table-4.1: Cyber Crime Incidents Records

Cyber attacks / crimes Incidents	**July-Dec-2018**	**Jan-June-2019**	**Increase /Decrease**
Cyber Harassment	565	784	+219
Online Fraud	5786	5964	+178
Spam	654	697	+43
Content related	756	798	+42
Vulnerability Reports	73	55	-18
Intrusion Attempts	5151	4671	-480

Denial of Services	345	296	-49

*Source: Reports from National Crime Record Bureau-2019



*Note: the above graph has a scale of 1 unit=1000pts

Interpretation:

As we can see in the above table, it's clear that certain cyber-crimes such as Cyber Harassment (up by 219), Online frauds (up by 178), spams (up by 43), and Content related cybercrimes (up by 42) have increased while on the other hand cyber-crimes like massive decrease in Intrusion attempts (down by 480), denial of services attacks (down by 49), and vulnerability reports (down by 18) is observed.

This proves that a lot of organizations and companies have started using the A.I. techniques to protect themselves against cyber-crimes. The organizations are now paying more attention towards securing their data, and thus they inherit, trade, and buy the ever-evolving A.I. techniques for the same [18].

4. FUTURE ISSUES CONSIDERATION

We should always be aware of the thin line difference between the immediate objectives or goals and the long run objectives and viewpoints, when we predict the usage and expansion of the A.I. field in the Cyber security domain. Most of the A.I. techniques seem relevant for

prevention against cyber assaults on the other hand, some complicated cyber techniques are required to fight against more complex cyber assaults [19].

We can observe the emerging new standards of knowledge and their utilization dealing with decision making procedures. These standards incorporate a totally modular and hierarchal knowledge architecture for software. Thus, for ensuring the leaders a decision superiority and decision makers a C2 level security fast enhancements of circumstance evaluation is used and only provided by automated knowledge management [20].

CONCLUSION

AI is considered as a standout amongst the most encouraging advancement in the information age and cyber security. New techniques, algorithm, tools and enterprises offering AI based services are always rising with respect to the worldwide security showcase. Contrasted with traditional cyber security solutions, these frameworks are more adaptable, flexible and robust, therefore enhancing security execution and better protect system from an expanding number of refined cyber threats. Right now, profound learning procedures are potentially the most encouraging and effective tools in the domain of AI. There is additionally an earnest requirement for use of intelligent cyber defence methods in a various area where the most appropriate technology is not only neural nets. As of recently, neither individuals nor AI alone have demonstrated general achievement in cyber security. Regardless of the immense change that AI has conveyed to the domain of cyber security, related frameworks are not yet ready to alter completely and consequently to changes in their condition. In addition, a holistic view on the cyber environment of associations is required.

REFERENCES

1. *The Role of Artificial Intelligence in Cyber Security January 2019, In book: Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems (pp.170-192)*
2. *Artificial Intelligence in Cyber Defense, January 2011, Enn tyugu*
3. *ARTIFICIAL INTELLIGENCE AND CYBER SECURITY – FACE TO FACE WITH CYBER ATTACK – A MALTESE CASE OF RISK MANAGEMENT APPROACH [Volume 9, Issue2(22) 2020]*

4. *JOUR Goztepe, Kerim 2012/01/01 13 19 Designing Fuzzy Rule Based Expert System for Cyber Security International Journal of Information Security Science*
5. *Akhmetov B., Lakhno V., Akhmetov B., Alimseitova Z. (2019) Development of Sectoral Intellectualized Expert Systems and Decision-Making Support Systems in Cybersecurity. In: Silhavy R., Silhavy P., Prokopova Z. (eds) Intelligent Systems in Cybernetics and Automation Control Theory. CoMeSySo 2018. Advances in Intelligent Systems and Computing, vol 860. Springer, Cham.*
6. *Machine Learning for Cyber Defense and Attack DATA ANALYTICS 2018 : The Seventh International Conference on Data Analytic.*
7. *AI-Driven Cyber Security Analytics and Privacy Protection Received 5 November 2019; Accepted 5 November 2019; Published 30 November 2019*
8. *Cyber security meets artificial intelligence: a survey. Published 2019, Computer Science Frontiers of Information Technology & Electronic Engineering*
9. *B.iftikhar, A.S.alghamdi, , "Application of artificial neural network in detection of dos attacks,"*
10. *Karpathy, A., Toderici, G., Shetty, S., Leung, T., Sukthankar, R., Fei-Fei, L.: Largescale video classification with convolutional neural networks. In: Computer Vision and Pattern Recognition (CVPR), 2014 IEEE Conference on. pp. 1725–1732. IEEE (2014)*
11. *D. Cire¸san, U. Meier, and J. Schmidhuber. Multi-column deep neural networks for image classification. Arxiv preprint arXiv:1202.2745, 2012*
12. *LeCun, Y., Boser, B., Denker, J.S., Henderson, D., Howard, R.E., Hubbard, W., Jackel, L.D.: Backpropagation applied to handwritten zip code recognition. Neural computation 1(4), 541–551 (1989)*
13. *LeCun, Y., Bottou, L., Bengio, Y., Haffner, P.: Gradient-based learning applied to document recognition. Proceedings of the IEEE 86(11), 2278–2324 (1998)*
14. *Nebauer, C.: Evaluation of convolutional neural networks for visual recognition. Neural Networks, IEEE Transactions on 9(4), 685–696 (1998)*
15. *2014 6th International Conference on Cyber Confl ict P.Brangetto, M.Maybaum, J.Stinissen (Eds.) 2014 © NATO CCD COE Publications, Tallinn Artificial (Intelligent) Agents and Active Cyber Defence: Policy Implications Caitríona H. Heinl Research Fellow Centre of Excellence for National Security (CENS) S. Rajaratnam School of International Studies Singapore*
16. *Rishabh Das, Thomas Morris, 2017/12/01 1 7 Machine Learning and Cyber Security 10.1109/ICCECE.2017.8526232*
17. *SELF-ORGANISING MAPS IN COMPUTER SECURITY Jan Feyereisl1and Uwe Aickelin The University of Nottingham Nottingham, UK*
18. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 10, OCTOBER 2020 ISSN 2277-8616 165 IJSTR©2020 www.ijstr.org Survey On The*

Applications Of Artificial Intelligence In Cyber Security Shidawa Baba Atiku, Achi Unimke Aaron, Goteng Kuwunidi Job, Fatima Shittu, Ismail Zahraddeen Yakubu

19. *Machine Learning Meets Communication Networks: Current Trends and Future Challenges JAZ AHMAD1, SHARIAR SHAHABUDDIN3, HASSAN MALIK4, ERKKI HARJULA2, TEEMU LEPPÄNEN2, LAURI LOVÉN2, ANTTI ANTTONEN1, ALI HASSAN SODHRO5, MUHAMMAD MAHTAB ALAM4, MARKKU JUNTTI2, ANTTI YLA-JAASKI6, THILO SAUTER7, ANDREI GURTOV5, MIKA YLIANTTILA2, JUKKA RIEKKI November 2020 IEEE Access PP(99) DOI:10.1109/ACCESS.2020.3041765*
20. *Artificial Intelligence and Cybersecurity: a promising but uncertain future Matteo E. Bonfanti. ARI 139/2020 - 9/12/2020*