2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. June 4-5, 2020

Enhancing Security Measures of AI Applications

Yuvraj Singh Chaudhry
Amity Institute of Information Technology
Amity University Noida
yuvi.chaudhry@gmail.com

Upasana Sharma
Amity Institute of Information Technology
Amity University Noida
usharma1@amity.edu

Ajay Rana
Amity Institute of Information Technology
Amity University Noida
ajay_rana@amity.edu

Abstract – **Artificial Intelligence also often referred to as machine learning is being labelled to as the future has been into light since more than a decade. Artificial Intelligence designated by the acronym AI has a vast scope of development and the developers have been working on with it constantly. AI is being associated with the existing objects in the world as well as with the ones that are about to arrive to improve them and make them more reliable. AI as it states in its name is intelligence, intelligence shown by the machines to work similar to humans and work on achieving the goals they are being provided with. Another application of AI could be to provide defenses against the present cyber threats, vehicle overrides etc. Also, AI might be intelligence but, in the end, it's still a bunch of codes, hence it is prone to be corrupted or misused by the world. To prevent the misuse of the technologies, it is necessary to deploy them with a sustainable defensive system as well. Obviously, there is going to be a default defense system but it is prone to be corrupted by the hackers or malfunctioning of the intelligence in certain scenarios which can result disastrous especially in case of Robotics. A proposal referred to as the "Guard Masking" has been offered in the following paper, to provide an alternative for securing Artificial Intelligence.**

Keywords— Artificial Intelligence, Applications, Cyber Security, Defenses, Future

I. INTRODUCTION

AI(Artificial intelligence) [2] is currently being referred to as the future. It is because this future is vast and has a lot of scope to improve daily lives of the people. AI is the intelligence that is actually the need of the hour. The algorithms that existed are starting to vanish, its due to the consecutive development in technology. The advancements in applications are not being able to run up on those existing algorithms or they function inefficiently. Artificial Intelligence can be the game changer for such issues. Teaching the machine itself to create solutions for the problems associated with applications.

The Intelligence itself needs algorithms to function and being able to support this perspective. So, instead of working separately on algorithms [3] for individual applications, people have been working upon to make the machines reliable by providing them with the intelligence, allowing them to grow similar to that of a human brain.

Since, the intelligence is always vulnerable to be corrupted by greed of others or self, it poses a big threat to the world. History states that, many intelligent have led to some disasters. Hence, the Artificial Intelligence can itself be a source for problems. These vulnerabilities may result in harming others. It can result to work oppositely than it is meant to be. It can result in data thefts, privacy invasion, executing wrongly in case of robots.

The vulnerabilities may arise due to the self-corruption of the intelligence or it might be manipulated by the Black Hats. It is important to take down these vulnerabilities to secure our future in reliable intelligence.

II. BACKGROUND

Artificial Intelligence is being regarded as the potential future we are looking forward to from a while. Development in AI has already given birth to a lot [1] of useful applications. These applications are improving and making our lives easier day by day. AI is evolving as we speak, and we have got no idea what heights it can reach. AI being a potential asset is itself might tend to be a threat if misused. AI's security mechanisms need to be improved as well with time, since the Black hats are also evolving as we speak. They are looking for new ways to infiltrate AI to get to its applications and corrupt them. Present defensive [4] measures are pretty good at holding AI's integrity. But they might get outdated very soon and improving them with version updates might not be enough. Working upon security of the applications is ought an challenge that is being continuously affecting the growth. It is the time to work upon a new style of defensive measures to protect AI as well as its applications.

III. APPLICATIONS

The applications of the AI are numbering up day by day. The existing applications are being evolved to meet up today's needs and for survival. AI is being the key factor in advancement of applications and inventing new technologies. New ideas are being implemented every day and many are being proposed and initiated. Some of the major applications being carried out currently are as follows:

A. Internet of Things

AI in IoT is enabling users to control their applications with more ease, providing them with a simple interface to interact on. AI has enabled all the applications to communicate with each other and understand the human commands more clearly to perform their tasks with an accuracy pleasing their users. AI has also adopted data mining for better functioning with IoT applications [1].

B. Training Programs

AI has made it possible to provide us with augmented reality and help humans prepare for new environments and challenges without actually entering them. It recreates the ideal situation with the collected data and help us to

978-1-7281-7016-9/20/$31.00 ©2020 IEEE

experience the situation beforehand, so that we are ready to face it properly when it is called for. ISS is an platform which trains astronauts with the help of AI before sending them into the new environment [2].

C. *Inheriting brain like Cognitive*

The Artificial Intelligence has finally started to mimic the human stimuli to an amazing extent. . It still haven't been able to mimic human stimuli completely but what has been already reached have provided a good alternative to problem solving. Human Inference System, also known as HIS model has played a major role in developing AI's stimuli [3]. It is done by recording the human stimuli and then trying to fuse it off with the AI by converting the computed data into algorithms and so. These algorithms have resulted in sharpening the intelligence and allow the AI to perform efficiently in many scenarios.

D. *Robotics*

Another sector in which AI has helped in, would be helping in build efficient robots. Robots have been under development from a long time and they have advanced a lot. The catalyst in this advancement would be AI, since, AI enables the robots to act more human like while performing tasks. Many robots have been developed in fields such as Medical to help out the doctors with difficult surgeries.

E. *Deep **Neural Networks***

A machine's recognition capabilities are getting accurate these days. It has also been possible because of the AI. AI has developed the DNN's to such an extent that the machines are being able to recognize an object, organism accurately. It has proven to recognize objects better than a naked eye in certain scenarios. There are many variants of recognizing processes. One such method is the Random pixel selection and then generating the image around it [4].

F. ***Medical** Purposes*

Recently there have been many cases of failures at surgeries. These failures have pointed out the need for improved surgical systems. AI has provided the alternative to reduce these failures. It has resulted in teaching machines to act as an helping hand to doctors [5]. AI Applications that is robots are being programmed to perform some of the difficult operations. It has already been deployed in the field. Moreover it has already started showing positive results.

G. *UAV –*

Unmanned Vehicles have provided the world to explore regions which are physically inaccessible or dangerous to the human kind. UAV's are been in use for a long time whether from the military sides or by the scientists to explore. The new UAV's are being encrypted by the Artificial Intelligence, so that they are able to access the new regions with more ease and work efficiently [6]. AI can operate the UAV's similarly to those as humans, maybe even more efficiently.

IV. Is AI really the future?

We often come across as Artificial Intelligence being said to be the future. But the question is why is it considered to be the future? The simple answer would be because of its vast domain to improve itself and improve the world's technology. We have already seen some of the applications of the AI above. Those applications are themselves the proof of effectiveness of AI. The above applications are just a fraction of what AI has to offer. AI has given life to many applications. It wouldn't be a mistake to consider that AI can be implemented with everything, because it really can be implemented with everything.

Moreover it is important to keep this future bright and prevent it from turning into darkness. These applications are open to vulnerabilities that can be exploited by the Black Hats to manipulate the functioning of its applications or to misuse them for greediness. AI needs to have a reliable defense system just not to protect the applications being controlled by it but to protect its intelligence as well from corrupting and leading to disasters.

V. AI's Role in Cyber Security

The Cyber Security has been statistically improved with the implementation of AI in its processes. AI learns the attacking mechanism inherited by the Black Hats. After learning the mechanism, it runs to itself detect the vulnerabilities used by the hackers to exploit the systems. If the vulnerabilities are detected then they can be closed before they are exploited. In case vulnerabilities are not detected, the AI looks for the similar attacking patterns used in the past and if a such pattern is detected by the intelligence, the counter measures to eliminate threats are deployed right away.

AI has been able to reduce Frauds, Scams, Phising, Data Thefts on a huge scale. It has been discussed in various conferences to improve domains of cyber security. One such discussion is already being implemented which seeks to recognize the malicious behavior with the help of neural networks and then execute the counter measures [7]. These malicious behavior are more tend to occur in systems operating on Windows due to the large area of vulnerabilities. The proposed architecture of a malicious behavior system in [7] is as followed in the diagram:

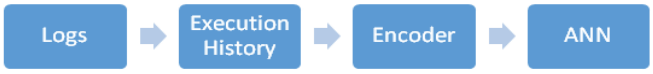

Fig. 1. Malware Behavioral System Architecture [7]

The Cyber security has been also improved by using of different and reliable algorithms in AI. Also, data mining is done using AI to increase security [8].

AI's another concept for improving security already discussed in previous conferences is of detection of Low-rate distributed denial of service using TCP connection parameters at the application layer [9]. LDDoS attacks are ought to be very stealthy and difficult to detect. The existing techniques used to detect LDDoS haven't been effective. So, it was proposed in [9] to detect the LDDoS attacks by considering in the characteristics of TCP to be the key differentiator. The proposal's test was impressive.

VI. Issues with Applications Security

Defensive measures being deployed with AI Applications to reserve the applications integrity has always been an area looked into, and the deployed measures have been effective so far. But there exists a loophole which occurs due to the overlooking of the security mechanisms for the algorithms being used up or the AI's own security itself. The current default security mechanism for such is vulnerable. These

vulnerabilities can result in corruption of the running algorithms and the functioning of the AI which in turn affects the functioning of the applications. These vulnerabilities can not only disarm the AI but also can handover AI's control to the hackers. If the control of AI gets handed over to the hackers, they can manipulate the functioning of the application. Or worse it can perform normally like its meant to be but the data being collected is being shared by unauthorized people as in case of a bank system, such as a person has just opened a bank account and have registered for net banking, but the bank system's security has already been infiltrated since the AI being deployed in its authentication has already been manipulated. The unauthorized personnel can use up the details of the users without being known to the users or the bank.

Another way by which the AI can be disarmed is by keeping AI engaged at a platform which is actually not the attack target. Such as the hackers before attacking up their actual target, can distract the target's AI and its security measures by attacking the source of AI, that is the hackers might attack AI's own defenses with DDoS or other hacking techniques to make it appear as if the target is being attacked by infiltrating the AI first but instead its just a decoy to keep AI's algorithms engaged in deploying counter measures for itself instead of keeping an eye on the application that its supporting. Let's look at a diagram for a better understanding at the concept.

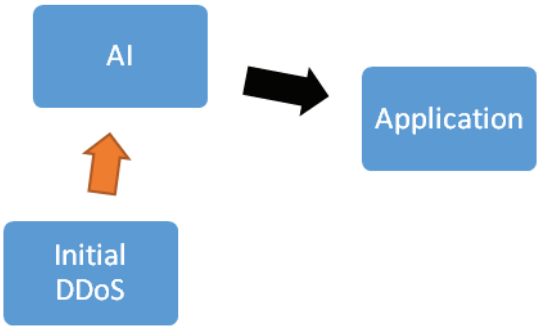

Fig. 2.

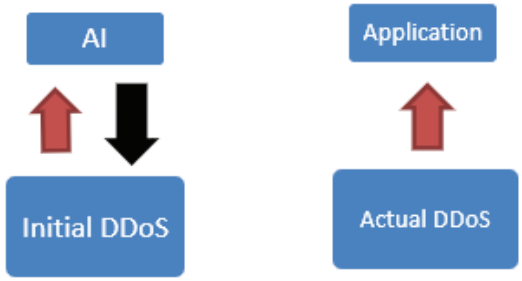

Fig. 3. Misguiding AI and creating vulnerability

VII. Proposed Technique

We would like to propose an idea as an alternative for such problems. We have named the following proposal as "Guard Masking" An option to resolve such issues could be developing another AI side by side with a core AI for the application. In this way we can minimize the core AI's complexity for providing security to itself as well. The core AI's objective would be to provide security against attacks just to its application. Now, this way the core AI is vulnerable to corruption as well as manipulation. Here's when the new AI comes handy. The other AI's sole purpose would be to provide security to core AI as well to itself. This AI will act as the guardian whose solo task is to protect itself and others. This guardian AI will be linked to the core AI through masking so that its source remains untraceable. Hence, even if the Black hats wants to infiltrate the core AI, they will first need to infiltrate the guardian AI, which would be very difficult as masking would be guarding its source, hence always misguiding the hackers to find its vulnerabilities.

The issue that comes up with this proposal is that the two AI's will be required to be in touch with a network all the time, so that the masking can take place. To overcome this problem, we all would need to come up and work together to find its solution. By combining all of our knowledge we just won't be able to strengthen this idea but also might be able to come up with much better and strong options in regard of this issue as well as the others.

Here is a diagrammatic representation of the proposal:

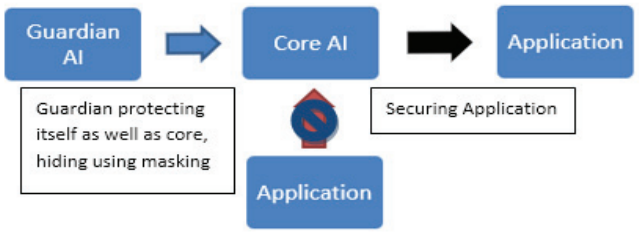

Fig. 4. Representation of Guardian and Core AI

VIII. Conclusions

Artificial Intelligence, its blooming itself brings threats to its integrity, as the hackers often tend to penetrate into things improving human life. Its an important concern to maintain its integrity and secure it, to avoid any dangers. Its applications are large in numbers and many more are coming day by day to help better our lives. AI is also responsible for providing security in many fields these days, protecting our data, our identity and our work.

A small manipulation in the algorithms could lead to corruption of AI which is dangerous and may result in drastic events. Hence, it calls for a need to work upon its own defensive measures as well, in order to make it stable and to maintain its integrity.

There's a need to invent new techniques and mechanisms to secure AI and our data. Guard Masking is so far just a concept which might be a stable possible resolution for the time. The concept can not be implemented right away and needs to be worked upon a bit more before moving ahead with it.

Our future plans involve implementation of Guard-masking properly. Currently its merely a concept which requires a lot of modifications before being brought into action. In future we are not just going to work upon evolving Guard Masking but also spend time in gathering more information about the holes in security measures in order to develop something more stable and secured. We are always open for suggestions and help in implementation of the concept.

REFERENCES

[1] Abdulhafis Abdulazeez Osuwa, Esosa Blessing Ekhoragbon, and Lai Tian Fat, *Application of Artificial Intelligence in Internet of Things*, 19 March 2018, https://ieeexplore.ieee.org/document/8319379

[2] Andrey Kuritsyn, Maxim Kharlamov, Sergei Prokhorov, and Dmitry Shcherbinin, *Application of Artificial Intelligence Systems in the Process of Crew Training*, 28 March 2019, https://ieeexplore.ieee.org/document/8674440

[3] Adang Suwandi Ahmad, *Brain Inspired Cognitive Artificial Intelligence for Knowledge Extraction and Intelligent Instrumentation System*, 11 January 2018, https://ieeexplore.ieee.org/document/8253363

[4] Seetarama Raju Pericherla, Nithish Duvvuru, and Dinesh Babu Jayagopi, *Improving Adversarial Images Using Activation Maps*, 5 August 2019, https://ieeexplore.ieee.org/document/8785543

[5] Yang Liu, and Pinpin Tang, *The prospect for the application of the surgical navigation system based on artificial intelligence and augmented reality*, 17 January 2019, https://ieeexplore.ieee.org/document/8613675

[6] Chethan Chithapuram, Yogananda V. Jeppu, and Ch. Aswani Kumar, *Artificial Intelligence Guidance for Unmanned Aerial Vehicles in Three Dimensional Space*, 26 January 2015, https://ieeexplore.ieee.org/document/7019634

[7] Cristian Pascariu, and Ionut-Daniel Barbu, *Dynamic analysis of malware using artificial neural networks*, 7 December 2017, https://ieeexplore.ieee.org/document/8166505

[8] Sagar B.S, Niranjan S, Nitin Kashyap, and Sachin D.N, *Providing Cyber Security using Artificial Intelligence – A survey*, 29 August 2019, https://ieeexplore.ieee.org/document/8819719

[9] Michael Siracusano, Stavros Shiaeles, and Bogdan Ghita, *Detection of LDDoS Attacks Based on TCP Connection Parameters*, 7 February 2019, https://ieeexplore.ieee.org/document/8635701

[10] Rosalind W. Picard, *Robots with Emotional Intelligence*, 2 August 2012, https://ieeexplore.ieee.org/document/6256094

[11] Narendra Kumar, Nidhi Kharkwal, Rashi Kohli, and Shakeeluddin Choudhary, *Ethical Aspects and Future of Artificial Intelligence*, 15 August 2016, https://ieeexplore.ieee.org/document/7542339

[12] RONALD C. ARKIN, *Ethical Robots in Warfare*, 16 March 2019, https://ieeexplore.ieee.org/document/4799405

[13] Li Mei, and Feng Cheng, *The use of artificial intelligence in the Information Retrieval System Epoch-making changes in information retrieval system*, 3 June 2010, https://ieeexplore.ieee.org/document/5477649

[14] Hu Shuijing, *The Influence of Artificial Intelligence Development on Patent Legislation*, 22 August 2019, https://ieeexplore.ieee.org/document/8806576

[15] Divanshi Priyadarshni Wangoo, *Artificial Intelligence Techniques in Software Engineering for Automated Software Reuse and Design*, 29 July 2019, https://ieeexplore.ieee.org/document/8777584

[16] Sonakshi Ruhela, *Thematic Correlation of Human Cognition and Artificial Intelligence*, 29 April 2019, https://ieeexplore.ieee.org/document/8701337

[17] LI Hua-Song, and KANG Wen-Xiong, Artificial Intelligence Tracing of Inherence Leakage Current between Power Line and Earth, 3 December 2010, https://ieeexplore.ieee.org/document/5656456

[18] https://www.normshield.com/cyber-security-with-artificial-intelligence-in-10-question/

[19] B. Dayal Chauhan B, A. Rana, N. K. Sharma, "Impact of development methodology on cost & risk for development projects", in 2017 6th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2017, pp 267-272 (2018).

[20] S. Chawla, G. Dubey, A. Rana, "Product opinion mining using sentiment analysis on smartphone reviews", in 2017 6th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2017, pp 377-383 (2018).

[21] H. Walia, A. Rana, V. Kansal, "A Naïve Bayes Approach for working on Gurmukhi Word Sense Disambiguation", in 2017 6th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2017, pp 432-435 (2018).

[22] D. Gupta, A. Rana, S. Tyagi, "A novel representative dataset generation approach for big data using hybrid Cuckoo search", in International Journal of Advances in Soft Computing and its Applications, Vol. 10, Issue 1, pp 55-70 (2018).

[23] S. Ghosh, A. Rana, V. Kansal, "A Nonlinear Manifold Detection based Model for Software Defect Prediction", in Procedia Computer Science, Vol. 132, pp 581-594 (2018).

[24] N. Agarwal, A. Rana, J. P. Pandey, "Fine-grained access control and secured data sharing in cloud computing", in Advances in Intelligent Systems and Computing, Vol. 729, pp 201- 214 (2018).

[25] A. Saroliya, U. Mishra, A. Rana, "Performance Evaluation and Statistical Analysis of AUR-Chord Algorithm with Default Working of Structured P2P Overlay Network", in Advances in Intelligent Systems and Computing, Vol. 583, pp 753-760 (2018).

[26] D. Gupta, A. Rana, S. Tyagi, "Sequence generation of test case using pairwise approach methodology", in Advances in Intelligent Systems and Computing , Vol.554, pp 79-85 (2018).