BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
http://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Human-Centered A.I. and Security Primitives

Alex Mathew*

Department of Cybersecurity, Bethany College, USA

ARTICLE INFO

Article history
Received: 9 November 2020
Accepted: 20 November 2020
Published Online: 30 November 2020

Keywords:
Artificial Intelligence
Deep learning
Digital signatures
Machine learning
Private information retrieval

ABSTRACT

The paper reviews how human-centered artificial intelligence and security primitive have influenced life in the modern world and how it's useful in the future. Human-centered A.I. has enhanced our capabilities by the way of intelligence, human informed technology. It has created a technology that has made machines and computer intelligently carry their function. The security primitive has enhanced the safety of the data and increased accessibility of data from anywhere regardless of the password is known. This has improved personalized customer activities and filled the gap between the human-machine. This has been successful due to the usage of heuristics which solve belowems by experimental, support vector machine which evaluates and group the data, natural language processing systems which change speech to language. The results of this will lead to image recognition, games, speech recognition, translation, and answering questions. In conclusion, human-centered A.I. and security primitives is an advanced mode of technology that uses statistical mathematical models that provides tools to perform certain work. The results keep on advancing and spreading with years and it will be common in our lives.

1. Introduction

Artificial intelligence (AI) is the study and design of algorithms that perform tasks or behaviors that a person could reasonably deem to require intelligence if a human were to do it [1]. Many mature technologies nowadays adopted by the general public have historically switched their design approaches from machine-centered to human-centered [2]. Increased digitization in various spheres of life has led to a shift towards the implementation of digital technologies for data management and administration [3]. The business sector offering A.I. services benefits the most from the importance of Human-Centered A.I. Programmers are directed to ensure a continuous flow of income from the user, meaning that humans have to be dependent upon the software in a certain sense.

Artificial Intelligence is of three different types:

(1) Narrow or Weak A.I.

(2) General or Strong A.I.

(3) Artificial Superintelligence

Current progressing improvements draw scientists closer to achieving general AI with several theories speculating its future where intelligent killer robots will take over the world by either wiping out the human race or enslaving all humanity. The optimistic theory relates a blending co-relation between humans and robots, where humans use artificial intelligence as a tool to enhance their life experience. These machines' speed and accuracy are already gaining root in human lives, performing tasks that would

**Corresponding Author:*
Alex Mathew,
Department of Cybersecurity, Bethany College, USA;
Email: Dr.alex.soh@gmail.com

DOI: https://doi.org/10.30564/jcsr.v2i4.2534

have otherwise been impossible for humans to complete independently.

However, humans' creativity and emotions are incredibly unique, that it becomes challenging for any programmer to replicate the machines' traits. Security Primitive is also an essential part of the A. I since it determines whether the selected portions of the image match with the password and also provides random access to the selected image if the password of the user is known. It refers to an integrated protocol within the software where specific procedural steps have to be taken before to accomplish an intended purpose. For example, a person may commit to a chosen value while keeping it hidden from others, with the ability to reveal it later. Even so, no one should trust the artificial system by default. Verification procedures that allow testing the AI "black box" behavior and outputs using different solutions already available should comply with legislation [4].

2. Proposed Methodology

This research paper's methodology section portrays the steps that can be followed to identify our current position with artificial intelligence. Understanding the primitives is a secure way of grasping the root of artificial intelligence.

3. Commonly Used Security Primitives

3.1 Digital Signatures

A digital signature is a mathematically designed scheme meant to verify the authenticity of digital documents. Once the digital prerequisites have been satisfied, the recipient will have no reason to doubt whether the known sender created the message and if its integrity was not altered during transit. It is implemented by having all scanners in, say, an office setting, sign each scan, and have the signature verified by the viewing applications to avoid fraud as any alteration is detected [5].

3.2 Private Information Retrieval

A file from a given server can be retrieved without leaving a trace of the database from where it was initially. It is particularly useful where the user cannot access the other information from the same database. The only possible protocol that can grant the user information-theoretic privacy is when the entire copy of the database is sent to them. Clients want to know that the servers perform correctly, to understand the reasoning behind their actions, and to know how to use them appropriately to guarantee safety of their information [6].

3.3 Mix Networks

Mix networks refer to complicated protocols created by hard-to-trace routing in a chain of proxy servers called mixes. The secret of a Mix Network is that it takes messages from multiple senders then sends them back at a random order to the next destination. The whole process becomes hard to trace since the link between the source and the goal is destroyed.

3.4 Algorithm

The three different steps in this research are:

(1) Supervised Learning

Programs set in the model with unrelated data are compared with the actual target outputs; therefore, minimizing errors. There are six kinds of supervised learning classifiers: random forest, gradient boosting machine, conditional random forest, naive Bayes, neural network, and support vector machine [7].

(2) Unsupervised Learning

Unsupervised learning is essentially incomprehensible without inductive biases both on the considered learning approaches and the data sets [8].

(3) Reinforcement Learning

Artificial neural networks are under the heading of regression and clustering algorithms, which either can fall under supervised or unsupervised methods. Reinforcement Learning is used in virtual games, in building collaborative multi-agent systems [9]. Virtual reality increases the performance of training due to immersion and realistic spatial objects [10].

Flow charts:

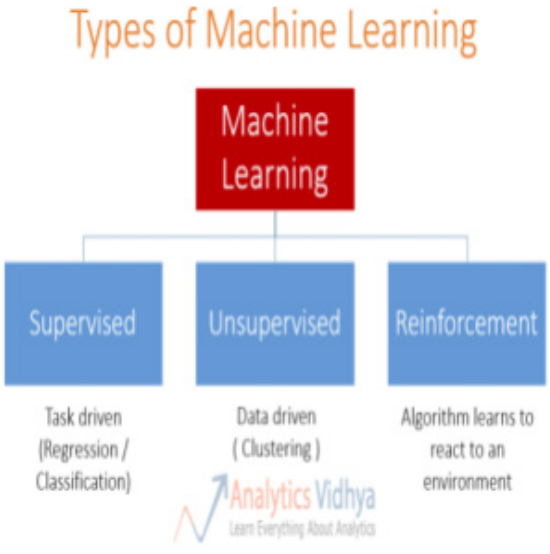

Figure 1. Types of Machine Learning algorithms

Source: https://www.analyticsvidhya.com/blog/2015/06/machine-learning-basics/

DOI: https://doi.org/10.30564/jcsr.v2i4.2534

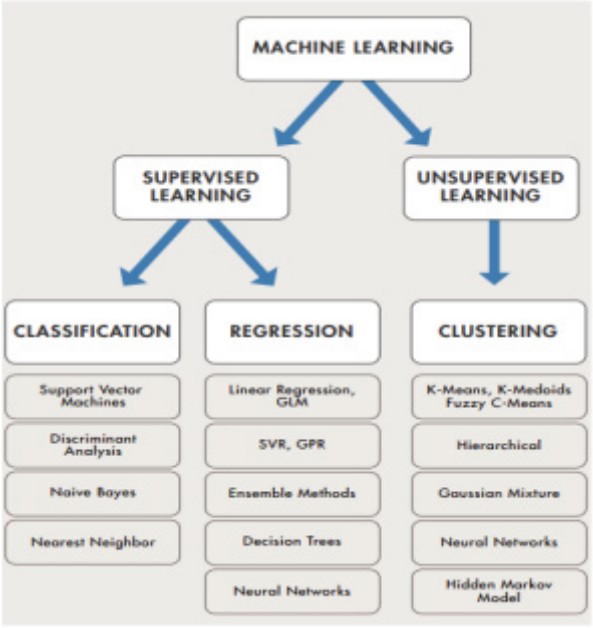

Figure 2. A summary of traditional machine learning methods

Source: http://www.datasciencecentral.com/profiles/blogs/machine-learning-summarized-in-one-picture

4. Result Analysis and Discussion

A more in-depth evaluation of the subject of artificial intelligence reveals ideas, thought, ambitions, and desires of man to progress to a higher level of human achievement. The world's rapid advancement towards an artificial future comes with worries and fear. The accuracy level of man is not infallible. Therefore, some loopholes may still prevail causing massive destruction at the epitome of the advancement. Below, the future of Artificial Intelligence and the possibilities of merits or demerits associated with it is discussed.

4.1 Artificial Narrow Intelligence (ANI)

The 21st century celebrates its achievement in this level of artificial progress. If a 19th-century corpse could resurrect today, it would be stunned by the rapid progress in technology vivid in this generation. Phones operated by fingerprints and unlocked by facial recognition are common advancements that a large population enjoys today. All credit goes to the obedient programs that are set to accomplish the given tasks. Narrow A.I. fitly pictures the constraints that the machines have been put to operate on. Human intelligence is here not replicated, but it merely simulates human behavior under a narrow set of parameters. Systems that excel at specific tasks, yet cannot apply their resources outside fairly narrow domains are said to have this Artificial Narrow Intelligence [11]. Examples of Narrow A.I. include:

(1) Self-driving cars
(2) Siri by Apple and other virtual assistants
(3) Email spam filters
(4) Disease prediction tools
(5) Face recognition software

Despite all its advantages, the selection of AI in numerous ventures is seen as a danger to low-and-middle talented specialists, as it will radically chop down dependence on the human labor force. The increasing level of unemployment created by the replacement of human labor by these machines is alarming and companies could gain a disproportionate advantage over conventional companies that still depend on normal, shift-based systems leading to unfair competition [12].

4.2 Artificial General Intelligence

The goal of AGI is the capacity to solve multiple problems, not just one [13]. Advanced AI, can mirror human behavior, and at times make conversations with humans forming relationships. This is capable of breaking the fabric holding the society as we know it.

4.3 Artificial Super Intelligence

Artificial Super Intelligence is the capability of human-made systems that can surpass humans [14]. The machine acts naturally mindful and goes past human insight and capacities. The ASI has a better memory and faster ability to process data. The reasoning and decision making of ASI will also be higher than that of humans. The thought of having such kind of machines sound appealing, especially when we imagine that we shall be sitting somewhere relaxed as we command the "non-exhausted humans" with ease. It is this level of technological achievement that scientists are busy striving to attain. The thought of the ASI taking over the dominion of man is also a speculated potential danger. Positively, malware identification techniques are used to improve cognitively-inspired inference [15].

5. Conclusion

Will the Artificial Super Intelligent level of technological advancement ever be achieved? In case it is completed, what of the accelerated hacking, A.I. terrorism, and more negative issues will be associated with them? Such questions and more may crisscross the mind of a thinker and possibly stigmatize the mind of a pessimist. If the current machines can still find their way to the hands of terrorists, the militia groups may even use the advanced devices for

DOI: https://doi.org/10.30564/jcsr.v2i4.2534

evil. A thought like this poses a danger to the forthcoming generations. It appears more profitable to appreciate the level of advancement we have attained and think of how humanity can benefit from it other than focusing on the higher. In contrast, society suffers from them.

References

[1] M. O. Riedl. Human-centered artificial intelligence and machine learning. Hum. Behav. Emerg. Technol., 2019, 1(1): 33-36.

[2] E. Coronado, G. Venture, N. Yamanobe. Applying Kansei/Affective Engineering Methodologies in the Design of Social and Service Robots: A Systematic Review. Int. J. Soc. Robot., 2020.

[3] G. Leiras. European Journal of Public Health. 2020, 3(5): 2020.

[4] A. Zorins, P. Grabusts. Safety of artificial superintelligence. Vide. Tehnol. Resur. - Environ. Technol. Resour., 2019, 2: 180-183.

[5] P. Hunter. The advent of AI and deep learning in diagnostics and imaging. EMBO Rep., 2019, 20(7): 1-4.

[6] B. W. Israelsen, N. R. Ahmed. "Dave...I can assure you ...that it's going to be all right ..." A Definition, Case for, and Survey of Algorithmic Assurances in Human-Autonomy Trust Relationships. ACM Comput. Surv., 2019, 51(6): 1-37.

[7] K. Mizukami et al. Genetic characterization of pancreatic cancer patients and prediction of carrier status of germline pathogenic variants in cancer-predisposing genes. EBioMedicine, 2020, 60: 103033.

[8] F. Locatello et al. Challenging common assumptions in the unsupervised learning of disentangled representations. RML@ICLR 2019 Work. - Reprod. Mach. Learn., 2019.

[9] L. Han et al. Grid-wise control for multi-agent reinforcement learning in video game AI. 36th Int. Conf. Mach. Learn. ICML 2019, 2019: 4558-4571.

[10] I. Petukhov, L. Steshina, A. Glazyrin, D. Velev. Design Model of a Training Simulator in Virtual Reality. FASSI 2019 Fifth Int. Conf. Fundam. Adv. Softw. Syst. Integr., 2019: 1-7.

[11] H. Shevlin, K. Vold, M. Crosby, M. Halina. The limits of machine intelligence. EMBO Rep., 2019, 20(10): 1-5.

[12] S. M. Abdullah. Artificial Intelligence (Ai) and Its Associated Ethical Issues. Islam Civilisational Renew., 2019, 10(1): 124-126.

[13] R. Thawonmas, J. Togelius, G. N. Yannakakis. Artificial General Intelligence in Games : Where Play Meets Design and User Experience. NII Shonan Meet., 2019, 130.

[14] M. L. How. Future-ready strategic oversight of multiple artificial superintelligence-enabled adaptive learning systems via human-centric explainable ai-empowered predictive optimizations of educational outcomes. Big Data Cogn. Comput., 2019, 3(3): 1-43.

[15] R. Thomson, C. Lebiere, S. Bennati, P. Shakarian, E. Nunes. Malware identification using cognitively-inspired inference. 24th Conf. Behav. Represent. Model. Simulation, BRiMS 2015, co-located with Int. Soc. Comput. Behav. Model. Predict. Conf. SBP 2015, 2015: 18-25.

 DOI: https://doi.org/10.30564/jcsr.v2i4.2534