DEEPFAKES AND WHAT COMES WITH IT.

INTRODUCTION:

Artificial Intelligence, a broad scientific subject that aims to understand and construct systems that exhibit intelligence-like traits, with origins in philosophy, mathematics, and computer science. In today's world, artificial intelligence (AI) is a huge field devoted to understanding and developing systems with intelligence-like characteristics, one of which is the ability to learn: the ability to extract information from inputs. This is a wide definition that coincides with existing statistical approaches in certain aspects. The present rush in progress in this field is due to a subset of AI, machine learning, and deep learning, in which computers are trained to discover associations based on massive volumes of raw data, such as the pixels of digital pictures, video content, tabular data, and so on. With roots in philosophy, mathematics, and computer science, this diverse scientific field aims to understand and build systems that display intelligence-like characteristics.

Technological growth has reached a new height, with even more potential to reach higher levels and attain larger goals. Artificial neural networks and deep learning artificial intelligence are rapidly evolving, owing to AI's ability to analyse enormous volumes of data considerably faster and generate more accurate predictions than humans. While the massive amount of data collected every day would bury a human researcher, AI solutions that use machine learning can swiftly turn that data into meaningful knowledge. (Dick, 2019)

SCOPE OF ARTIFICIAL INTELLIGENCE:

Top scientists and business leaders like Stephen Hawking and Bill Gates have warned that the rise of Smart Technology, Artificial Intelligence, Robotics, and Algorithms, or STARA, will result in mass unemployment. By 2025, it is projected that STARA will have taken one-third of all occupations currently available. This is due to considerable advancements in robotic dexterity and intelligence, as well as the availability of low-cost autonomous units capable of outperforming humans in a variety of physical and conceptual activities.

Artificial intelligence is said to be playing an increasingly important role in educational technology, management sciences, and operational research. Intelligence is often defined as the ability to gather information to solve complex situations. In many domains, intelligent machines will soon be able to replace human talents. Artificial intelligence (AI) has progressed to the point that it can now provide real-world benefits in a variety of applications. Expert systems, intelligent computer-aided instructions, natural language processing, speech comprehension, robotics, and sensory systems, computer vision and scene identification, and neural computing are some of the major artificial intelligence areas. These expert systems have given rise to a rapidly evolving technology that is having a significant impact on a variety of fields. (Mittal & Sharma, 2021)

Furthermore, the healthcare industry is one significant sector that will benefit from technological advancements and AI. Artificial Intelligence is expected to diagnose and treat patients, execute vital operations, and make complicated judgments, allowing them to recover faster than before.

CONTROVERSIES OF ARTIFICIAL INTELLIGENCE:

Artificial intelligence, according to its critics, poses an existential threat to humans on multiple levels. From a philosophical and ethical standpoint, opponents have raised worry that attempts to simulate human thought could jeopardize the singularity of human consciousness, potentially resulting in catastrophic consequences. Many of these disastrous outcomes have inspired dystopian science fiction, with authors exploring post-apocalyptic realities caused by artificial intelligence that has evolved into "superintelligent" and hence independent. As a result of its autonomy, machinery may pose a threat to human survival. More immediate worries raised by critics include the potential that growing automated machinery in numerous industries would eventually replace human employees, resulting in mass unemployment, as well as the risk of machine-learning algorithms containing inherent racial and socioeconomic bias.

The superfluous inclusion of human-like elements in public AI technology The superfluous inclusion of human-like elements in public AI technology presentations, such as natural-sounding voices, facial expressions, and simulated displays of human emotions, reinforces this anthropomorphic illusion. Each of these strategies has a place in human-computer interfaces, but not when their main purpose is to deceive or deceive. Attempts to garnish significant AI achievements with humanoid flourishes do a disservice to the field by

creating unnecessary questions and hinting that there is more to it than meets the eye. Synthetic media and deepfakes enter the picture at this point. (Kaplan, 2016)

SYNTHETIC MEDIA AND DEEPFAKES:

Artificial intelligence (AI) breakthroughs are enabling new types of misdirection. AI algorithms can create realistic "deepfake" videos, as well as fake photographs and writing that look real. These methods, together known as synthetic media, have sparked considerable alarm about their ability to spread political disinformation. However, the same technology can be used to cause financial harm. The first publicly reported incidents of deepfakes being used for fraud and extortion have surfaced in recent months. Synthetic media is a new type of media that is posing a growing threat to international security.

Deepfakes are artificial intelligence-generated media that realistically represent made-up events. "Deepfake" is a slang phrase that has no technical definition. It most frequently refers to a person saying or doing something they never said or did on film or audio. Deepfakes are made using deep learning, an AI technique. It is based on a deep neural network, a complex computing system loosely modeled after biological brains. The network first takes in training data of a person's face, then uses an algorithm to derive mathematical patterns from it. The network can create new, synthetic representations of the target's face or speech based on these patterns. A face-swap film, which transposes one person's facial motions onto the features of another, is the best sort of deepfake. Voice cloning is another sort of deepfake, in which a person's distinctive vocal patterns are copied to digitally replicate and change their speech. A face-swap film, which transposes one person's facial motions onto the features of another, is the most well-known sort of deepfake. (In 2017, internet users began transposing female celebrities' faces onto other faces in pornographic films, coining the name "deepfake."). Voice cloning is another sort of deepfake, in which a person's distinctive vocal patterns are copied to digitally replicate and alter their speech. (Bill, 2021c)

The line between actual and fake media has gotten increasingly blurred. On the one hand, this offers up a slew of new possibilities in industries like creative arts, advertising, film production, and video gaming. On the other side, it offers a significant security risk. Free software packages available on the internet enable anyone with no special expertise to generate extremely convincing fake photos and films. These can be used to sway public opinion in elections, perpetrate fraud, defame, or blackmail individuals. (*Media Forensics and DeepFakes: An Overview*, 2020)

ETHICAL ISSUES CONCERNING SYNTHETIC MEDIA AND DEEPFAKES:

Deepfake technology poses several ethical issues. With the ability to create realistic-looking and sounding video or audio files of people doing or saying things they didn't do or say, deception has never been easier. Concerns regarding its potential use for blackmail, intimidation, and sabotage, ideological persuasion, and incitement to violence, as well as broader implications for trust and responsibility, are raised in the literature that addresses the ethical implications of deepfakes. While this research is crucial in identifying and signaling the potentially far-reaching repercussions, the moral dimensions of deepfake technology and deepfakes themselves receive less attention.

If a technology violates moral norms (following deontology), has significant negative consequences that outweigh its positive effects (following consequentialism), weakens virtue and/or promotes vice (following virtue ethics), or undermines interpersonal relations and fundamental social values like trust and mutual respect (following virtue ethics), it may be considered morally wrong (following care ethics). Deepfake technology appears to be a morally problematic technology at first glance. Its very name implies that it has anything to do with deception. A device that deceives by making phony footage looks to be morally questionable. Deception, after all, breaches truthfulness norms, instills erroneous beliefs, is a vice, and is destructive to social interactions and trust. (Ruiter, 2021)

DEEPFAKES IN THE COOPERATE WORLD:

Deepfake technology has made it more difficult to distinguish between genuine and fake media, posing a danger to businesses. You can combat counterfeit media head-on with the correct training, identification, and reaction strategy. Deepfake, which is a mix of the phrases "deep learning" and "fake," is an AI-based system that creates or modifies images, audio, and video to produce synthetic content that appears legitimate. This can range from imitating a voice over the phone (to sound like a CEO or CFO requesting a money transfer) to conveying a convincing likeness on film. It can be changed in real-time or on tape. With the world becoming more linked through digital media and the cost of making deepfakes plummeting, this burgeoning technology poses a severe threat to your company. In this post, we'll go over the dangers of this technology and, more importantly, how you can protect your company from them. (Debusmann, 2021)

Beyond the maturation of technology, the risk of deepfakes is heightened by the fact that, as a result of COVID-19, workplaces have become virtual overnight. This type of digital transformation boosts the usage of video conferencing and other digital office tools, which means greater access to deepfake material and more chances of being duped. Deepfakes fall into two categories when it comes to the threats they offer to businesses: The act of influencing individuals to execute malevolent actions, such as revealing confidential information, is known as social engineering. This could involve duping an employee into transferring funds using phony audio or video. Deepfake technology has already been used to successfully carry out high-profile scams. A UK energy executive was conned out of £200,000 in 2019 after receiving a phony phone call from his employer requesting that he transmit emergency funds.

Fake films of CEOs and other powerful people giving false information about a company can impact public perception. When complaints go unanswered, it can harm a company's brand, influence consumer behavior, and even affect the stock price. (Simonite, 2020)

PRECAUTIONS AGAINST DEEPFAKES:

We've gathered specialists from both our Security and Applied Intelligence practices to assist outline an appropriate reaction to the increasing deepfake danger. We've developed a simple methodology that you can use to help prepare for the impact of harmful deepfake attacks as a result of this diverse effort. (Ding et al., 2021)

Three pillars support this methodology:

1. Employee training and awareness - Employees can be turned into an extra line of defines by providing sufficient training and raising awareness. Employees should be trained on how to recognize deepfake-based social engineering attempts and how to detect how the technology is used in malevolent attempts. With great success, we've used a similar concept at clients to help prevent the threat of email-based phishing through security awareness initiatives.
2. Model of detection - While perfect risk mitigation is difficult, early detection of false media can assist reduce the impact on your organization. We've teamed up with entrepreneurs to create models that can spot phony photos and videos. This is especially important for combating bad actors' attempts to sway public opinion with deepfakes.

3. Ensure that your business is prepared to respond appropriately in the event of a deepfake. Prepare a plan that can be implemented if a deepfake is found. Individual duties and needed actions must be clearly outlined in this strategy.

("The Deepfake Challenges and Deepfake Video Detection," 2020)

REFERENCES:

- Dick, S. (2019, July 1). *Artificial Intelligence · Issue 1.1, Summer 2019*. Harvard Data Science Review. https://hdsr.mitpress.mit.edu/pub/0aytgrau/release/2
- Mittal, U., & Sharma, D. M. (2021). Artificial Intelligence and its Application in Different Areas of Indian Economy. *International Journal of Advanced Research in Science, Communication and Technology*, 160–163. https://doi.org/10.48175/ijarsct-v2-i3-328
- Kaplan, J. (2016). Artificial intelligence. *Communications of the ACM*, *60*(1), 36–38. https://doi.org/10.1145/2950039
- Bill, B. (2021c, October 11). *Synthetic Media: How deepfakes could soon change our world - 60 Minutes*. CBS News. https://www.cbsnews.com/news/deepfake-artificial-intelligence-60-minutes-2021-10-10/
- *Media Forensics and DeepFakes: An Overview*. (2020, August 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/9115874
- Ruiter, D. A. (2021, June 10). *The Distinct Wrong of Deepfakes*. SpringerLink. https://link.springer.com/article/10.1007/s13347-021-00459-2?error=cookies_not_supported&code=223d867f-8bfb-48c1-bf13-e161cd1238d4
- Debusmann, B. B., Jr. (2021, March 8). *"Deepfake is the future of content creation."* BBC News. https://www.bbc.com/news/business-56278411
- Simonite, T. (2020, July 7). *Deepfakes Are Becoming the Hot New Corporate Training Tool*. Wired. https://www.wired.com/story/covid-drives-real-businesses-deepfake-technology/
- The Deepfake Challenges and Deepfake Video Detection. (2020). *International Journal of Innovative Technology and Exploring Engineering*, *9*(6), 789–796. https://doi.org/10.35940/ijitee.e2779.049620

- Ding, F., Zhu, G., Li, Y., Zhang, X., Atrey, P. K., & Lyu, S. (2021). Anti-Forensics for Face Swapping Videos via Adversarial Training. *IEEE Transactions on Multimedia*, 1. https://doi.org/10.1109/tmm.2021.3098422