1. Describe the relationships between Big Data, AI and Machine Learning.

Big data refers to large, fast, and complex datasets that are impractical to process using traditional methods. It originates from various sources, including transactions, smart IoT devices, industrial equipment, multimedia content, and social media interactions. Big data serves as the foundational material for Artificial Intelligence (AI) and Machine Learning (ML) applications. Machine Learning involves using computational methods to leverage experience, improve performance, or make predictions. Conversely, AI is a branch of technology that creates intelligent computer programs capable of tasks requiring human-like intelligence. Big data is crucial for training Machine learning models to make accurate predictions. AI then uses these models developed by ML to perform tasks that come very close to human perceptions and adapt to the new data. To explain this relationship, let's take two examples. Firstly, in the healthcare sector, a vast volume of data is generated daily, encompassing lab results, patient records, prescription histories, and new medications. Processing this data using traditional methods is unfeasible, highlighting the importance of Big data technologies. Using Machine Learning, patterns and models can be developed to provide valuable insights, such as correlations between disease phases and effective treatments. When integrated into AI systems, these models enable the adaptation to new information and the ability to make predictions. To draw another analogy, let’s use human learning: as children, we are surrounded by new information that we don’t know how to process. This represents Big Data. We learn new things with time and start drawing connections between them to find patterns. That is like Machine Learning. Once we start learning more, we can make predictions on how to react to new situations, how to learn new information, and how to interact with unknown problems. That is like Artificial Intelligence.

References

Big Data Analytics: What it is and why it matters. SAS. (n.d.-b).

Kaplan, J. (2016). Artificial intelligence: What everyone needs to know. Oxford University

Mohri, M., Rostamizadeh, A., & Talwalkar, A. (2018). Foundations of machine learning. MIT

Panesar, A. (2019). Machine learning and AI for healthcare (pp. 1-73). Coventry, UK: Apress.

2. Explain the core differences between Strong AI and Weak AI. How could strong AI pose a future security threat?

Strong Artificial Intelligence refers to a system with general intelligence comparable to human cognitive abilities. Just as humans can learn and perform intellectual tasks, strong AI is envisioned to exhibit similar capabilities. However, it raises questions about the potential emergence of consciousness. In contrast, Weak AI is designed for specific tasks and lacks the capacity for self-awareness and abstract reasoning. Familiar examples include virtual assistants like Siri or Alexa. Currently, true Strong AI remains a theoretical concept and is not realized even by advanced models like Chat-GPT, which excel in processing and generating information based on patterns but lack innate human cognitive capacities. If Strong AI were to become a reality, it could potentially pose security threats, particularly in the realm of autonomous decision-making. Strong AI might develop a sense of autonomy and decision-making ability, potentially conflicting with human interests. If provided with incorrect or misleading information, it could take unexpected actions, posing risks to security and human well-being. Furthermore, there's concern that Strong AI could evolve beyond human control. For instance, if tasked with optimizing financial algorithms, it might modify its own processes to pursue maximum financial gain, inadvertently leaving systems that have been used vulnerable to exploitation by malicious actors and resulting in security incidents. Strong AI can also be a deadly weapon when it comes to being used by Nation Actors with the sole benefit of causing chaos. Imagine this scenario where Nation Actors use strong AI to generate cyberattacks. Drawing from military experiences, AI decided to impersonate its attack as it was coming from a different source, causing confusion and escalated tension between nations. It is important to recognize that, much like any human invention, the development of Strong AI requires global cooperation. It is crucial to understand that there are dual potentials within Strong AI: one for benevolent applications and another with the potential for harm.

References

B. T. M. A., Authors, Centre, T. M. C. R., Trend Micro, Centre, C. R., Us, C., & Subscribe. (2023, August 15). Top 10 AI security risks according to OWASP. Trend Micro.

Flowers, J. C. (2019, March). Strong and Weak AI: Deweyan Considerations. In AAAI spring symposium: Towards conscious AI systems (Vol. 2287, No. 7).

Ng, G. W., & Leung, W. C. (2020). Strong artificial intelligence and consciousness. Journal of Artificial Intelligence and Consciousness, 7(01), 63-72.

AI security threats: The real risk behind science fiction scenarios. Security Intelligence. (2023, October 24).