In recent years, the field of data science has experienced a tremendous transformation. The growth in data volume and complexity has resulted in the emergence of big data in many industries thus evolving new data processing methods and data analysis. Given the proliferation of data and the industries' search for new business patterns to improve decision-making, data science and the demand for data scientists have begun to grow greatly (Dataquest, 2021).

Data science advances in the field of big data as artificial intelligence thrives on data to learn, automates repetitive tasks, and parses decision-making. Cybersecurity becomes critical in addressing the security and privacy challenges associated with large data. Understanding, analyzing, and processing data would be crucial for identifying risks and vulnerabilities and fortifying defenses to prevent security breaches. Potential security breaches can be identified by analyzing the security logs for data/file transfer, operational, authentication/authorization errors. Using Neural networks, Artificial Intelligence and Machine Learning algorithms can be trained on such big datasets to detect and prevent events in real-time. By using artificial intelligence to learn about network traffic patterns and behaviors, network security may be enhanced in locations where sensitive data is stored (Costa, 2022). There are multiple factors influencing convergence in cybersecurity, thus obtaining algorithm-agnostic convergence being the desired outcome in the future (Hero et al., 2023)

Although there are various opportunities, limitations, and challenges, the convergence of the field does indeed promise a transformative future. Data-driven models can provide deeper insight and exposure through the analysis of big data. However, as technology and data continue to evolve, privacy and security start can become a significant problem. Human decision-makers rely on data that has been processed, cleaned, analyzed, and transformed; thus, when enormous amounts of data are fed into Artificial Intelligence systems, their self-learning algorithms assist in complimenting human decision-making (Teboul, 2021). When trying to analyze patterns and behavior in the data, limitations in data quantity and quality might result in biased training for training data and real-time decision-making (Yooseff, 2019). It can be challenging to explain to businesses how data can benefit them, but persuading them to do so and demonstrating the significant effect that data can have on their decisions can help them see the usefulness of utilizing data to make more informed decisions.

References

Hero, A., Kar, S., Moura, J., Neil, J., Poor, H.V., Turcotte, M. and Xi, B. (2023). Statistics and Data Science for Cybersecurity. Issue 5.1, Winter 2023, 5(1). doi: https://doi.org/10.1162/99608f92.a42024d0.

Teboul, B. (2021). The challenges of the convergence of Data, AI, Cloud, Blockchain, IoT and Cybersecurity. European Scientist. Available at: https://www.europeanscientist.com/en/features/the-challenges-of-the-convergence-of-data-ai-cloud-blockchain-iot-and-cybersecurity/ [Accessed 12 November 2023].

Dataquest. (2021). The Past, Present, and Future of Data Science. Available at: https://www.dataquest.io/blog/evolution-of-data-science-growth-innovation/.

Yooseff, I. (2019) Data Science and Artificial Intelligence Opportunities and challenges, SAP Blogs. Available at: https://blogs.sap.com/2019/07/13/data-science-and-artificial-intelligence-opportunities-and-challenges/ [Accessed 13 November 2023].

Costa, E. (2022) Artificial Intelligence in cybersecurity: The Benefits and challenges, CENGN. Available at: https://www.cengn.ca/information-centre/innovation/artificial-intelligence-in-cybersecurity-the-benefits-and-challenges/ [Accessed 12 November 2023].