The surge in big data is propelled by the growing volume and diversity of data, necessitating businesses to engage in intricate data analysis, cleaning and transformation for uncovering new patterns and making improvements. However, errors in business decision-making may arise if data processing and analysis yield ineffective or deceptive outcomes (Cai and Zhu, 2015). Using neural networks, it enables AI to generate real-time outcomes, however it is crucial to acknowledge the constraints related to the quality and quantity of data influencing real-time decision-making.

Data quality may be improved through thorough validation and cleaning processes to ensure accuracy and reliability in data (Clements, 2023). Techniques like interpolation or duplication in data augmentation helps to overcome quantity constraints, creating a more robust dataset for training AI models. Consistent training and dataset updates enable the AI systems to adapt the changing circumstances, ultimately enhancing real-time decisions, improving business outcomes (Brownlee, 2021). Ethical concerns arise as people may disagree with the outcomes of ML algorithms. One of the most important steps in ensuring customer satisfaction is to encourage data scientists to provide businesses with the necessary transparency in the algorithms they utilize.

With data security and privacy becoming more pressing as data grows, businesses are required to anonymize and encrypt data in accordance with GDPR regulations, restricting access to vital information to ensure robust security in the data management of consumer data (LinkedIn, 2023).

A focused emphasis on cybersecurity is vital, as there is high escalation on security breaches. Analyzing security logs becomes crucial for monitoring network patterns, and AI and ML systems must be trained using extensive datasets. The training data gets increasingly skewed and complex as attackers discover new ways to exploit it. Acknowledging the limitations of biased training data is essential in mitigating security risks, emphasizing ethical standards, and holding data scientists accountable for implementing ethics into practice (Heer, 2023). Although it cannot halt an attack, this strategy aids in lowering the proportion of security breaches and informs the relevant stakeholders of the projected risk.

Looking ahead, AI and ML will play pivotal roles in revolutionizing cybersecurity, particularly in automating the compliance and governance process. This involves automated monitoring, reporting, and the identification of security rule breaches (Singh, 2023). The anticipation of an algorithm-agnostic convergence in the future is aimed at addressing diverse elements impacting cybersecurity (Hero et al., 2023), ensuring a secure digital future.

References

Brownlee, J. (2021). How to Update Neural Network Models With More Data - MachineLearningMastery.com. *MachineLearningMastery.com*. [online] 4 Mar. Available at: https://machinelearningmastery.com/update-neural-network-models-with-more-data/

Cai, L. and Zhu, Y. (2015). The Challenges of Data Quality and Data Quality Assessment in the Big Data Era. *Data Science Journal*, 14(0), p.2. doi: https://doi.org/10.5334/dsj-2015-002.

Clements, J., R, R. and Mos (2023) Data cleansing to enhance decision making, Managed Outsource Solutions. Available at: https://www.managedoutsource.com/blog/data-cleansing-supports-better-decision-making-business-outcomes/ [Accessed on 24 November 2023

Heer, S. (2023). Data Science in Cyber Security: Applications, Importance, Future. https://www.knowledgehut.com/blog/data-science/data-science-in-cyber-security. [Accessed on 26 November 2023].

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.

LinkedIn Community. (2023). How Can You Overcome Real-Time Marketing Data Limitations? https://www.linkedin.com/advice/0/how-can-you-overcome-real-time-marketing-data. [Accessed on 25 November 2023].

Singh, A.P. (2023). Future of AI and Machine Learning in Cybersecurity. [online] Analytics Vidhya. Available at: https://www.analyticsvidhya.com/blog/2023/02/future-of-ai-and-machine-learning-in-cybersecurity/.