Discussion Summary 1

The internet of things (IoT) is ever-expanding in terms of the number of interconnected devices, and the volume of data collected from such devices (Tejada, n.d.). This is thanks to it becoming increasingly possible to connect more and smaller devices to the network in a way that is both cost-effective and efficient (Rose et al, 2015). This can present a vast opportunity set for IoT users and businesses across a range of industries, particularly with advances in data analytics techniques to deal with the high volumes and velocity of data produced by IoT devices. Businesses are able to utilize this analysis to inform decision making by studying key trends, patterns, and anomalies from these data sets, as well as drive improvements in their products and services (IBM, n.d.).

On the other hand, while the interconnectivity of IoT devices presents increased opportunities, it can also bring limitations and risks. Rose et al. (2015) and WINIX Technologies (2018) highlight that a security breach in one poorly secured system can lead to all other connected devices on the network becoming vulnerable to attacks, which in the context of IoT can be quite severe. N-IX (2019) argues the catastrophic consequences of hackers successfully gaining access to public infrastructure such as smart cars and healthcare, while Bitdefender (2023) highlights the popularity of denial of service attacks. Furthermore, Rose et al. (2015) also highlights issues relating to device interoperability, particularly those from different manufacturers, where data may be produced in various formats, which can hinder data exchange and device integration. Finally, Tejada (n.d.) argues that the complex big data architectures used for real-time analysis could lead to a trade-off between accuracy and timeliness, depending on the system and client needs.

Although the IoT currently has a number of drawbacks, there are ways addressing these to ensure the it remains viable. For example, the European Commission (2022) will require IoT devices sold within the EU to meet certain cybersecurity standards from 2025. Additionally, cloud services such as Google Cloud Armor can provide IoT networks with an added layer of security, protecting its devices from malicious attacks such as denial of service (Google Cloud, 2024). Finally, addressing the issue of accuracy vs. timeliness, innovative architectures such as fog computing, can be used to reduce latency and improve connectivity (Andrade et al., 2021).

References

Andrade, E., Nogueira, B., Farias Júnior, I. de & Araújo, D. (2021) Performance and Availability Trade-Offs in Fog–Cloud IoT Environments. *Journal of Network and Systems Management* 29(1). DOI: https://doi.org/10.1007/s10922-020-09570-9

Bitdefender. (2023) The 2023 IoT Security Report. Available from: https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf?src_trk=em66b6ebe5bf2b72.382051341180644271 [Accessed 20 August 2024].

European Commission. (2022) Cyber Resilience Act. Available from: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act [Accessed 20 August 2024].
Google Cloud. (2024) Cloud Armor Documentation: Security Policy Review. Available from: https://cloud.google.com/armor/docs/security-policy-overview [Accessed 20 August 2024]

IBM. (n.d.) What is the Internet of Things (IoT)? Available from: https://www.ibm.com/topics/internet-of-things [Accessed 19 August 2024].

N-iX. (2019) Key IoT security issues and how to deal with them. Available from: https://medium.com/@N_iX/key-iot-security-issues-and-how-to-deal-with-them-82d11bb8343f [Accessed 20 August 2024].

Rose, K., Eldridge, S. & Chapin, L. (2015) *The Internet of Things: An Overview.* Geneva: Internet Society.

Tejada, Z. (n.d.) Big data architectures. Available from: https://learn.microsoft.com/en-us/azure/architecture/databases/guide/big-data-architectures [Accessed 19 August 2024].

WINX Technologies. (2018) 6 Main Challenges Facing IoT. Available from: https://medium.com/@winix/6-main-challenges-facing-iot-b6055bdf6782 [Accessed 20 August 2024].