COLLABORATIVE DISCUSSION 1: THE DATA COLLECTION PROCESS

INITIAL POST

Mahir Hashimov
12695120
Unit 1-3
Deciphering Big Data
University of Essex Online
24 May 2024

INITIAL POST

There are a lot of prospects for increased productivity, automation, and innovation with the Internet of Things (IoT). Large volumes of data are generated by IoT devices, which improve decision-making. Smart cities employ the IoT to enhance traffic management and save energy usage, while wearable sensors provide continuous monitoring in the healthcare industry, facilitating the early identification of health problems and customised treatment plans (Gubbi et al., 2013).

IoT has several drawbacks, such as problems with data interoperability brought on by a lack of standardised protocols between systems and devices. Seamless data integration and analysis are hampered by this fragmentation. In addition, as Huxley et al. (2020) point out, a significant amount of infrastructure is required to manage the enormous data flood from IoT devices, necessitating sophisticated big data architectures and cloud services.

IoT security and privacy pose significant dangers. Cyberattacks may result in unauthorised access and service interruptions on devices. IoT decentralisation hampers security efforts and makes it challenging to apply standard security solutions. Constant data collection also presents privacy issues as users might not be conscious of the volume of information being collected or how it will be used (Roman et al., 2013).

There are many obstacles involved in implementing IoT on a large basis. Extensive planning and resources are needed for the effective lifecycle management of IoT devices. Since different devices may create contradictory data in different contexts, it is important to ensure data quality and dependability. Efficient stream processing systems, like Azure Stream Analytics or Apache Kafka, are necessary for real-time data processing in order to manage high-throughput data with minimal latency (Zaslavsky et al., 2013).

The idea behind IoT is that it can link disparate systems and devices, which may lead to data-driven innovation and improved operational efficiency. For IoT deployment to be effective, it is imperative to address constraints, risks, and problems. To fully utilise IoT across industries, advanced big data architectures, strong security frameworks, and standardised protocols are necessary.

References:

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660. DOI: 10.1016/j.future.2013.01.010

Huxley, K., 2020. Data Cleaning. ebook. SAGE Publications Limited. ISBN 9781529748147, 1529748143.

Roman, R., Najera, P., & Lopez, J. (2013). Securing the Internet of Things. Computer, 44(9), 51-58. DOI: 10.1109/MC.2011.291

Zaslavsky, A., Perera, C., & Georgakopoulos, D. (2013). Sensing as a service and big data. International Conference on Advances in Cloud Computing (ACC), 21-29. DOI: 10.48550/arXiv.1301.0159