Miraim Enokpa
University of Maryland Global Campus
Computer Networks & Cybersecurity

The Internet of Things (IOT) concept was first proposed in 1999 in the Auto-ID laboratory at Massachusetts Institute of Technology. This concept's primary idea is to provide a connection to the internet for all items to attain intelligent recognition and proper management of networks. This connection is provided using sensors like Radio Frequency Identification, which depends on a network of wireless sensors network and a radio frequency identification technology. The Internet of Things has since been established as a system of interrelated computing devices that possess unique identifiers (UIDs) and the capacity of transferring data over a network without needing and human interference in the interaction.

The IoT network consists of smart devices enabled on the web using embedded systems, such as sensors, processors, and communication hardware, to gather, disseminate and act on data they need from their various environments. The IoT network devices share the collected sensor data by connecting to an IoT gateway or any other edge device where data is either analyzed locally or sent to the cloud (Iera et al., 2010). Due to the limited human interaction, these devices pose the capabilities of acting on the information they receive from each other. Although the general concept of IoT is the same, the networking, connectivity, and communication protocols on a device largely depend on the application deployed.

The internet has been used in numerous applications throughout different sectors, proving the importance of this technology in daily living in both work and home settings. IoT has proven to be essential to businesses as they provide them with a detailed outlook of how their systems work. Companies can also benefit from the automated processes as they reduce any wastage, reduce labor costs, improve service delivery, and bring total transparency to monetary transactions. As much as the technology is aimed at improving living systems and doing business, it has two sides to it. There are both benefits and disadvantages. The benefits include:

- Giving users the ability to access information on any device from any location.
- It establishes improved communication between devices that are connected electronically.
- The technology saves time and money as data packets are transferred to a connected network.
- Contributes to improving the quality of a business's services as human error are reduced due to the lack of human interference.

The disadvantages also include:

- It increases the chance of hackers gaining access to sensitive information. It would only need them to hack into one device to access all devices' data in the network.
- Organizations continue to adopt the technology; they will eventually challenge all the collected data.

- If one device has a bug, the others in the system are all likely to get corrupted.

Despite the challenges faced by adopting this technology, different sectors continue to use it in numerous applications. The manufacturing and industrial sector have seen IoT adoption in the automotive and energy industries (Shrouf & Miragliotta, 2015). The consumer segment has various applications, from adopting IoT in big industries such as the housing industries through smart buildings to devices such as wearable devices that monitor an individual's vitals. The healthcare industry has also profited widely in IoT technology as it has brought benefits to both patient care and hospital administration work. Patients can now be monitored closely without being in the hospitals, and the massive data files regarding patients' history are now managed more effectively.

IoT continues to be adopted in various sectors. However, there is still the issue of vulnerabilities and attacks that continue to threaten its success, and this a primary concern due to its broad attack surface. Although some measures have been put in place, some attacks have been successful, like the Mirai, a botnet of 2016 that affected multiple websites for some time (Antonakakis et al., 2017). Despite the vulnerabilities it presents, IoT has proven to be one of the essential technologies in the world today in everyday life. Like another emerging technology, it continues to go through further advancements to ensure it realizes its full potential.

References

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Kumar, D. (2017). Understanding the Mirai botnet. In *26th {USENIX} security symposium ({USENIX} Security 17)* (pp. 1093-1110).

Iera, A., Floerkemeier, C., Mitsugi, J., & Morabito, G. (2010). The internet of things [guest editorial]. *IEEE Wireless Communications*, *17*(6), 8-9.

Shrouf, F., & Miragliotta, G. (2015). Energy management based on Internet of Things: practices and framework for adoption in production management. *Journal of Cleaner Production*, *100*, 235-246. https://doi.org/10.1016/j.jclepro.2015.03.055