Data Islands and IoT

Angela Milova

Palo Alto - Secure the Future

1. Describe two or more future IoT devices that would be expected in your sector.

The health sector would benefit greatly from future IoT devices, as once-fictional concepts have become tangible realities. In healthcare, IoT devices are anticipated to deliver innovative solutions, elevating patient care, refine diagnostics, and aiding healthcare workers in managing their workload more effectively. Some of the future IoT devices expected in the healthcare sector include: 1. Smart Pills: These are medications embedded with tiny ingestible sensors. Once ingested, these sensors activate, communicating data to an external device for doctors to analyze. Smart pills offer a better understanding of the patient's health, especially in cases of rare diseases. They also facilitate quicker and more personalized treatment, addressing current healthcare practice gaps. Moreover, in clinical trials, smart pills assist in more accurately tracking the effects and patient responses to new medications (Oza, 2023). 2. Smart Wearable Health Monitors: While some features of this technology are already present in smartwatches, future smart wearables have the potential to surpass traditional wearables. They can monitor and display real-time health metrics such as glucose levels, respiratory rate, ECG, etc. Smart wearables provide a holistic view of an individual's health, alerting users to potential issues before they become serious. They can guide individuals in the right direction when signs of potential health issues arise (Chawla, 2020). 3. Remote Patient Monitoring Implants and Data Analysis: Miniaturized IoT implants or sensors can be implanted within patients to monitor specific health conditions or vital signs continuously (ZenBusiness, 2023). These implants transmit real-time data to a system capable of conducting data analysis and providing the proper treatment or adjustments based on the collected data. This approach particularly benefits patients with limited hospital access, offering real-time and cost-effective treatment, especially for chronic conditions. Additionally, it assists healthcare staff in managing their workload more

efficiently by providing continuous patient monitoring (Appventurez, 2023). As these future IoT devices advance and seem so promising, ethical considerations, including patient privacy and consent, must be carefully addressed to ensure responsible and widespread adoption.

2. Specific to your industry sector, explain the complexities and/or failures associated with perimeter-based security.

Perimeter-based security in healthcare faces significant complexities and risks of failure. Several key challenges are associated with perimeter-based security in healthcare. 1. Distribution of Healthcare Systems - In healthcare, organizations are often geographically dispersed, with hospitals located in different areas and IT systems spread across various locations. This complexity raises the challenge of secure and effective communication among these entities, potentially leading to gaps in the perimeter and unauthorized access to patient data. 2. Digitalization of Healthcare - The increasing digitization of healthcare means that a wealth of information is now accessible online and through smartphone apps. This amplifies the risk of data leaks, emphasizing the importance of incorporating robust security measures in web development to ensure data confidentiality (Hurst, Boddy, Merabti, et. al, 2020). 3. Interconnected Medical Devices - The rising use of IoT devices in healthcare introduces complexity as these devices need to communicate with each other (Appventurez, 2023). The evolving nature of IoT devices necessitates continuous training for security teams to keep pace with emerging threats and changes in device technology. 4. Insider Threats - Insider threats pose a constant risk in the healthcare sector, where individuals within the organization may leak data to unauthorized users. Managing and monitoring user behavior adds an additional layer of complexity to perimeter-based security (Lee, 2022). 5. Advanced Persistent Threats (APTs) - Given the critical nature of the healthcare sector, it becomes a prime target for Advanced Persistent Threats (APTs) seeking financial gain and access to user data. With the rapid evolution of APTs, perimeter-based security may struggle to detect and mitigate these threats in a timely manner, leaving the healthcare sector vulnerable to the compromise of sensitive data

(Papastergiou, Mouratidis, Kalogeraki, 2021). Several measures need consideration to address these complexities and challenges, including implementing strong data encryption, multi-factor authentication, and powerful endpoint detection. Leveraging artificial intelligence (AI) for faster anomaly detection and proactive perimeter defense can be crucial in responding rapidly to potential security breaches. Additionally, regular audits, risk assessments, and ongoing staff training are essential components to ensure the effectiveness of perimeter-based security in healthcare (He, Aliyu, Evans, et. al, 2021).

References

Appventurez*, What is the future scope of IOT in Healthcare?*. (2023, November 1).

Chawla, N. (2020). AI, IOT and Wearable Technology for Smart Healthcare-A Review. *International Journal of Recent Research Aspects*, *7*(1)

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *Journal of medical Internet research*, *23*(4), e21747

Hurst, W., Boddy, A., Merabti, M., & Shone, N. (2020). Patient privacy violation detection in healthcare critical infrastructures: an investigation using density-based benchmarking. *Future Internet*, *12*(6), 100

Lee, I. (2022). Analysis of insider threats in the healthcare industry: a text mining approach. *Information*, *13*(9), 404.

Oza, H. *Future of IOT applications in Healthcare 2023*.

Papastergiou, S., Mouratidis, H., & Kalogeraki, E. M. (2021). Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. *Evolving Systems*, *12*.

ZenBusiness, T. (2023, November 24). *Future of IOT in Healthcare*. ZenBusiness Inc.