Brian Sowers

11/24/2023

Data Islands and IoT

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

"IoT in banking" refers to the interconnected network of IoT (Internet of Things) devices that gather, transmit, and process data, either in the cloud or on-premise servers, with the goal of enhancing the banking experience for both clients and bankers (Pandey, 1). In the near future, the financial sector is poised to witness the emergence of innovative IoT devices that promise to enhance the industry. One such advancement is the biometric ATM, which integrates IoT technology with biometric authentication methods to provide an exceptionally secure and convenient means of accessing banking services. Customers would utilize their biometric data, such as fingerprints or facial recognition, to perform transactions, eliminating the need for physical cards or PINs and greatly enhancing security. These ATMs would offer personalized services, and banks could monitor their status in real-time, ensuring their optimal functionality.

Additionally, fraud detection cards are set to continuously monitor cardholder activity and spending patterns, swiftly identifying and preventing fraudulent transactions. Equipped with IoT sensors and machine learning algorithms, they perform real-time analysis of customer financial data. Learning from cardholder behavior, these cards minimize false positives and offer real-time alerts for suspicious activity, empowering users to take immediate action. They can dynamically adapt security settings based on transaction patterns, ensuring adaptive security. As more data accumulates, fraud detection will improve further with enhanced machine learning

models. These IoT devices promise to reshape the financial sector, delivering improved customer service and security while adapting to the evolving industry landscape.

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

Perimeter-based security, a conventional approach to safeguarding data, reveals numerous complexities and potential failures when applied to the financial sector. The financial industry's highly sensitive data is a prime target for malicious actors, necessitating robust security measures. However, relying solely on perimeter-based security measures like firewalls and network boundaries has exhibited significant limitations. A startling statistic underlines these limitations: "Ninety-seven percent of financial apps tested in a six-week study lacked safeguards against revealing their source code" (Williams, 1). Furthermore, "Eighty percent of apps exhibited weak encryption algorithms or improperly implemented strong ciphers," (Williams, 1) increasing the risk of cached sensitive data being decrypted and manipulated. These alarming deficiencies in many financial apps exposes them to potential exploitation and underscore the pressing need for enhanced security measures within the financial industry.

Considering highly sensitive information frequently lives outside its own perimeter, this highlights the misconception that security measures can be one-size-fits-all, especially in the diverse and sensitive financial sector. It is evident many blind spots in security exist and a comprehensively tailored security approach is required to achieve data security. This approach may include the combination of data islands and their perimeter-based security, data integration restrictions, and a cloud security solution such as Palo Alto's Prisma. An example of a data island

in the financial sector may be a bank's siloed database for retail banking operations, investment services, or insurance offerings. It should be noted, however, that applications often replicate, cache, and move data to mobile and endpoint devices and that the data is only as secure as the location where they reside.

To address these limitations, Palo Alto's Prisma offers a superior alternative for network security in the financial sector. Prisma provides comprehensive protection by focusing on a data-centric approach. It goes beyond perimeter-based security, incorporating robust encryption, secure coding practices, and continuous monitoring. Moreover, Prisma facilitates routine security assessments and audits, identifying and rectifying vulnerabilities proactively. This ensures the safeguarding of sensitive financial information against emerging threats. In an ever-evolving digital landscape where financial services rely increasingly on mobile apps and digital platforms, Prisma offers the data-centric and proactive security measures indispensable for preserving the integrity and reliability of financial services (*Prisma*).

Works Cited

Pandey, Prachi. “What is IoT in Banking? Meaning, Advantages, Applications, and more.” *Sab Paisa.* https://sabpaisa.in/blog/iot-in banking/#:~:text=IoT%20in%20banking%20is%20the,for%20both%20clients%20and%20bankers. Accessed: 24 November 2023.

Prisma. *Palo Alto Networks TechDocs*. 2023. https://docs.paloaltonetworks.com/prisma. Accessed: 24 November 2023.

Williams, Robert. “Nearly all financial apps have security flaws that leave data vulnerable, study finds.” *Marketing Dive.* https://www.marketingdive.com/news/nearly-all-financial-apps-have-security-flaws-that-leave-data-vulnerable-s/551794/. Accessed: 24 November 2023.