

El Internet de las Cosas (IoT) es básicamente que todos los aparatos electrónicos —desde el refrigerador hasta los relojes inteligentes— estén conectados a internet, compartiendo datos todo el tiempo. La idea es que esto nos haga la vida más fácil. Pero para que funcione, se necesitan redes súper rápidas (como el 5G o los satélites de Starlink) y mucha seguridad. El problema es que, entre más dispositivos haya conectados (y ya son millones), más oportunidades hay para que los ciberdelincuentes roben información o saboteen sistemas, sobre todo si los fabricantes no ponen contraseñas seguras o no actualizan el software.

Además, el IoT tiene varios agujeros de seguridad: desde protocolos de comunicación poco confiables (como el Bluetooth o el WiFi) hasta errores humanos, como no cambiar las contraseñas o no instalar las actualizaciones. Los expertos están trabajando en soluciones, como usar inteligencia artificial para proteger los datos directamente en los dispositivos y no solo en la nube, pero aún hay mucho por mejorar. Al final, el IoT puede ser increíble, pero si no se maneja bien, también puede ser un desastre de privacidad y seguridad.

Escogí este artículo porque dentro de un futuro a mediano plazo para mi carrera creo que quiero especializarme en ciberseguridad entonces me decidí por este artículo, aun no estoy 100% sobre si esta sera la rama definitiva a la que me quiero dedicar pero lo quiero descubrir, también por eso me cambie a linux.