Skillmine
Technology ▪ Consulting ▪ Services

CYBERSECURITY

in the Age of IoT

skill-mine.com

TABLE OF CONTENTS

Cybersecurity and its Importance in IoT

According to Cybersecurity Intelligence, 2021 saw 50% more cyberattacks per week oncorporate networks compared to 2020. Most targeted sectors worldwide by hackers in 2021 include:

- Education/Research sector (up by 75%).
- Cyberattacks on the Healthcare sector (up by 71%).
- Internet Service Provider/Managed Service Provider (up by 67%).
- Communications (up by 51%).
- Government / Military sector (up by 47%).

According to Accenture's Cost of Cybercrime Study, 43% of cyberattacks are aimed at smallbusinesses, but only 14% are prepared to defend themselves.

Cybersecurity stands as the bedrock of our digital world, safeguarding systems, networks, and data from a rising tide of cyber threats. In the era of the Internet of Things (IoT), wherean ever-expanding array of devices and objects are seamlessly interconnected, the importance of cybersecurity has escalated to unprecedented levels.

What is Internet of Things (IoT)?

The term "Internet of Things," commonly known as IoT, pertains to the vast network ofcommon-place objects – ranging from smartphones and refrigerators to automobiles andmore – all inter connected via the Internet. This network facilitates the gathering and exchange of data among these objects, often referred to as "things."

Each device becomes a potential entry point, and any vulnerability in the system can have far-reach-ing consequences.

The interconnected nature of IoT means that a security breach in one device could potentially compromise an entire network, affecting both personal privacy and critical infrastructure.

The Internet of things

Any Place
Anywhere

Anything
Any Device

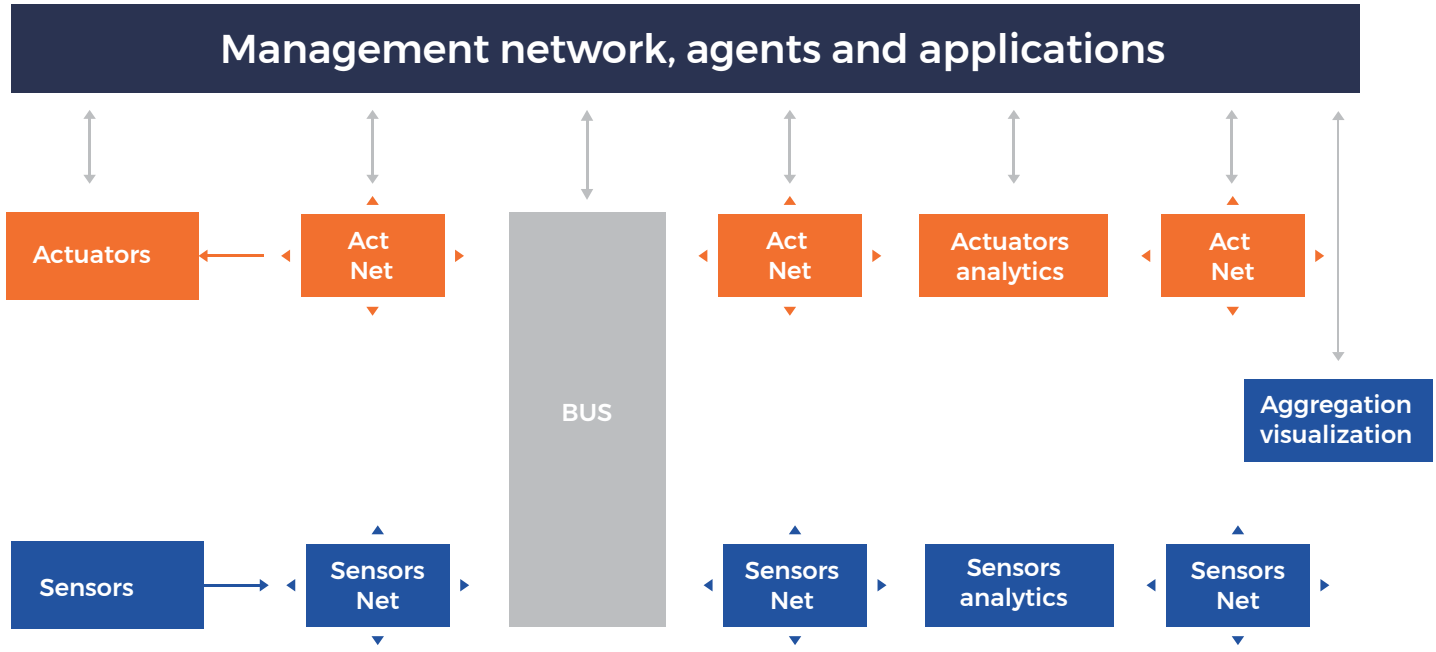
Anyone
Anybody

Any Service
Any Business

Any Path
Any Network

Anytime
Any Context

IoT security architecture components



IoT Architecture

In an IoT architecture, there exist four key layers, akin to the Open Systems Interconnection model, and can be elucidated from bottom to top:

1. Device Layer:

Representing the things translating the physical into digital, this layer comprises sensors and actuators. Devices, often numbering in the hundreds of thousands, connect to networks through wired or wireless means.

2. Network Layer:

Responsible for connecting IoT devices and facilitating data movement, this layer includes gateways and potential data aggregation methods. It ensures seamless communication between devices and computing resources.

3. Computing Layer:

This layer orchestrates local processing in IoT setups. Here, data is collected, stored, and initially analyzed, potentially involving edge computing for preprocessing. Local computing reduces network traffic, optimizing data center resources.

4. Application Layer:

At the pinnacle, this layer manages user interactions and serves as the hub for data analytics and reporting. While handling device management and environment control, the application layer integrates data from the computing layer, enabling comprehensive analytics and reporting in the primary data center.

As our physical surroundings become digitized and smart devices permeate every aspect of our daily life, ensuring robust cybersecurity measures becomes not just a matter of safeguarding data but also a crucial factor in maintaining the integrity, privacy, and safety of individuals, businesses, and even entire communities.

The age of IoT underscores the pressing need for a comprehensive and adaptive cybersecurity approach to mitigate risks, protect sensitive information, and uphold the trust that underpins the digital transformation of our world. This eBook will explore the ways to enhance cybersecurity in the Age of IoT.

How can you Ensure the Security of Your IoT Connections?

Steps to Enhance Security in the Age of IoT

In the realm of IoT, where various devices like smartphones, tech gadgets, and smart devicesseamlessly interconnect, neglecting adequate security measures can pave the way forunauthorized access.

The information generated by the Internet of Things (IoT) may contain sensitive and confidential details. Transmitting such data over open networks can pose risks of snooping, theft, and hacking. Organizations embarking on IoT projects must prioritize IoT privacy, implementing robust measures to secure devices and data both during transmission and in storage.

Employing encryption is a prevalent strategy for ensuring IoT data security. Furthermore, additional security measures are essential to thwart hacking attempts and prevent malicious alterations to device configurations. This comprehensive security approach encompasses a variety of software tools and traditional security devices, including firewalls and intrusion detection and prevention systems. Here are a few effective strategies for enhancing the security of your IoT connections:

Design: Choose IoT devices equipped with the most robust security features and integrate these features from the inception of any IoT design phase. Exercise equal diligence in strategizing and securing the associated IoT network environment, including the implementation of a distinct Wi-Fi network dedicated to IoT devices.

Process: Deploy tools, policies, and procedures to effectively identify and appropriately configure each IoT device, incorporating firmware upgrades when accessible. Avoid leaving any IoT devices "orphaned" by ensuring they do not rely on manual configuration or other forms of human intervention.

Diligence: Employ IoT management tools for the continuous monitoring and enforcement of IoT device configurations, complemented by security tools designed to identify intrusions or malware in IoT device deployments.

Despite these measures, IoT devices face various security risks, from botnet attacks to vulnerabilities in DNS systems, emphasizing the need for a vigilant approach to maintain compliance and protect sensitive data.

The landscape of IoT is in constant evolution, yet the absence of universally adopted standards for IoT infrastructure design, configuration, operation, and security persists. Businesses often rely on documenting decisions and correlating them with general IT best practices. While choosing IoT devices adhering to standards like IPv6 and connectivity standards provides a foundation, it may not be sufficient. Encouragingly, emerging compliance standards, such as IEEE 2413-2019, offer a common framework for diverse domains, reinforcing existing compliance postures in IoT implementation.

IoT security and compliance require seamless integration with broader IT-related initiatives, necessitating updates to guidelines and best practices across equipment, configurations, processes, and personnel management in alignment with IoT demands.

Bulletproof Your IoT Connections with Skillmine

Skillmine is a frontrunner in the IT and Tech industry, with a proven track record of delivering high-quality, effective, efficient, and user-friendly tech solutions. With our extensive grasp of cyber-security intricacies and profound industry acumen, we possess the capability to craft cutting-edge cybersecurity solutions that span the entire spectrum of services. Our cybersecurity services encom-pass consultation, implementation, and managed services. These comprehensive measures are meticulously designed to provide holistic protection for every facet of your business operations.

Drawing upon our well-rounded knowledge of cybersecurity, we strategize, execute, and oversee a range of services to ensure that your business remains safe-guarded from potential threats. By combining managed security services, advanced analytics, and intelligent automation, our cybersecurity solutions empow-er organizations to stay resilient

How Skillmine Enhanced IoT Security for a Smart Manufacturing Company?

A prominent player in the smart manufacturing industry, utilizing IoT devices and technologies faced growing concerns regarding the security of their interconnected devices and data. With an extensive network of IoT devices controlling critical manufacturing processes, the company needed a robust cybersecurity solution to protect its operationsfrom potential cyberattacks. The business approached Skillmine to address its IoT security concerns comprehensively.

Potential vulnerabilities in device configurations, data transmission protocols, and authentication mechanisms were identified by the Skillmine team. Based on the assessment, a customized security framework that encompassed end-to-end protection was devised. To prevent unauthorized access, MFA was implemented for all IoT device interactions. A real-time monitoring system was also set up to detect any abnormal activities or anomalies within the IoT network. Enhanced security mechanisms were added and physically consolidated but logically segregated network was made possible through segmentation.

By implementing these cybersecurity measures, the company experienced enhanced data protection and reduced vulnerabilities. The implementation of security measures ensured smooth and secure operations. The real-time monitoring system allowed the security team to detect and respond to potential threats before they could escalate.

In short, investing in cybersecurity services not only mitigated risks but also bolstered thecompany's reputation as a secure and reliable smart manufacturing provider.

For more information
Contact: info@skill-mine.com

Visit us: skill-mine.com

Stay connected