Best Practices for Cloud-Based IoT Security

by Satya K Vivek | April 11, 2023

Cloud-based IoT solutions are the future for digital products and services. However, the security risks associated with virtual infrastructures can't be ignored either. Cybercriminals are constantly finding new ways to carry out malicious attacks and call for tighter security practices. Thankfully, building IoT solutions on the cloud is a solution and can significantly bolster the network's security.

How can cloud computing address IoT security challenges?

Now, one might find this to be a little confusing. How can cloud computing help tackle IoT security challenges if moving your operations online opens new opportunities for cybercriminals? Well, an on-premises server would still be vulnerable to attacks. The leading cloud providers, on the other hand, provide the best security tools, practices, and processes. An organization's IoT data would be safer on a cloud-based infrastructure.

3 Most common security threats for cloud based IoT solutions.

Cyber criminals have a wide range of techniques at their disposal to exploit vulnerable networks. The most common security threats faced by cloud based IoT solutions include:

Data breaches - Most cyber-attacks result in unauthorized access or theft of data from a system – which is broadly known as a data breach. The data might include sensitive, confidential, or proprietary information such as credit card numbers, business details or financial details such as bank information etc.

Denial of service - Wreaking havoc against businesses and organizations of all sizes in 2022, the WannaCry Ransomware showed how devastating denial of service (DOS) attacks can be. These attacks intend to render a service inaccessible. A DOS attack on an IoT network can cause huge losses by bringing certain operations to a standstill.

Device hijacking - As the name suggests, device hijacking involves an attacker taking unauthorized control of a device – which could be anything from a smartphone to a large-scale factory system. Even by hijacking a single device, the attacker can potentially access sensitive information from the network or use it to launch attacks on other devices.

3 best security practices for cloud based IoT solutions.

When developing a cloud based IoT solution, make sure to implement the following security practices. The cloud provider of your choice should have them in place too.

Encryption

Encrypting your data makes it almost impossible to decipher without a decryption key, which only a limited number of people have access to. Thus, even in the event of a data breach, the attackers wouldn't be able to use the stolen information.

Network segmentation

This architectural approach involves dividing a network into several segments, also known as subnets. Traffic between the subnets is regulated by the network administrators, and security personnel can protect valuable assets like static IP addresses, highly confidential intellectual property assets, and customer data more effectively.

Multi-factor authentication

You can easily add new layers of security to an IoT network by introducing multi-factor authentication (MFA). It requires users to pass two or more verification processes before they can access a network or service. For instance, in addition to providing their account password, they might also be required to input an OTP or verify their identity using their fingerprint.

IoT solutions need to be bolstered with security practices.

Any IoT solution, be it a service offered to customers or an organization's in-house network, must incorporate the latest security practices. Regular audits and vulnerability assessments are necessary to maintain the effectiveness of the protective mechanisms and helps maintain IoT network's security and integrity.