केनरा बैंक Canara Bank
सिंडिकेट Syndicate

Advisory

IoT (Internet of Things) Security Challenges

What is IoT?

IoT refers to a system of interrelated, internet-connected objects that are able to collect and transfer data over a wireless network without human intervention.
Examples are smart watches, medical sensors, smart security systems, voice assistants, etc.

Why security of IoT devices are important?

- Most IoT devices operate unattended by humans, thus it is easy for an attacker to physically gain access to them.
- Most IoT components communicate over wireless networks where an attacker could obtain confidential information by eavesdropping.
- Most IoT components cannot support complex security schemes due to low power and computing resource capabilities.
- Anything from an employee device to a router connected to an unsecured network can put an entire organization's digital infrastructure at risk.

Tips to protect your IoT devices

Change Passwords often

Ensure that:

- each IoT device has a unique password which is strong and complex.
- change these passwords on regular intervals.

Avoid Universal plug & play feature

Once Universal Plug & Play is enabled, we need not configure every device on its own, and hence is more prone to outside attacks.

Don't rely on Cloud technology

An active connection is required to access data and files stored in cloud.
This connection can be hacked and is quite vulnerable to outside attacks.

Update your IoT device regularly

This installs security patches on your device(s) and stops hackers from using novel ways of intruding them.