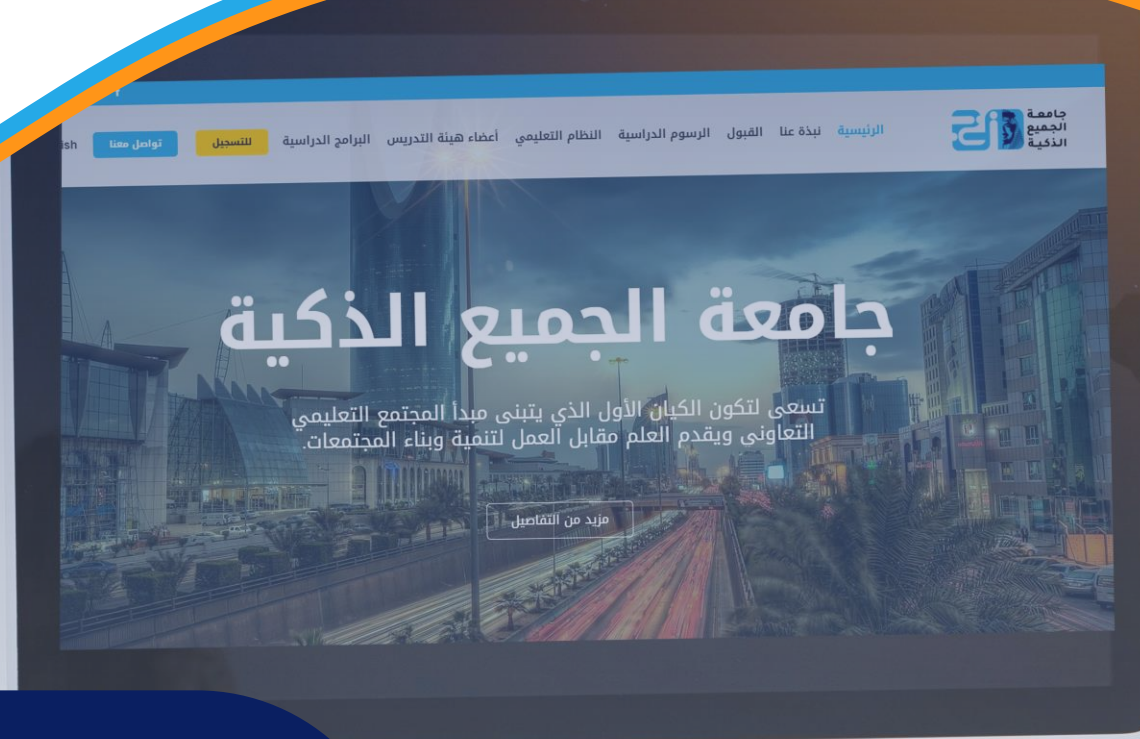




جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



IoT Security
Prepared by Dr. Abdelrhman Ahmed
Orientation Week

IoT Security Overview

The term **IoT, or Internet of Things**, refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud and between the devices themselves. Thanks to the advent of inexpensive computer chips and high bandwidth telecommunication, **we now have billions of devices connected to the internet**. This means everyday devices like toothbrushes, vacuums, cars, and machines can use sensors to collect data and respond intelligently to users.

The Internet of Things integrates everyday “things” with the internet. Computer Engineers have been adding sensors and processors to everyday objects since the 90s. However, progress was initially slow because the chips were big and bulky. Low power computer chips called RFID tags were first used to track expensive equipment. As computing devices shrank in size, these chips also became smaller, faster, and smarter over time.

Chapter 01

IoT Devices

IoT devices are pieces of hardware, such as sensors, actuators, gadgets, appliances, or machines, that are programmed for certain applications and can transmit data over the internet or other networks. They can be embedded into other mobile devices, industrial equipment, environmental sensors, medical devices, and more.

Internet Of Things

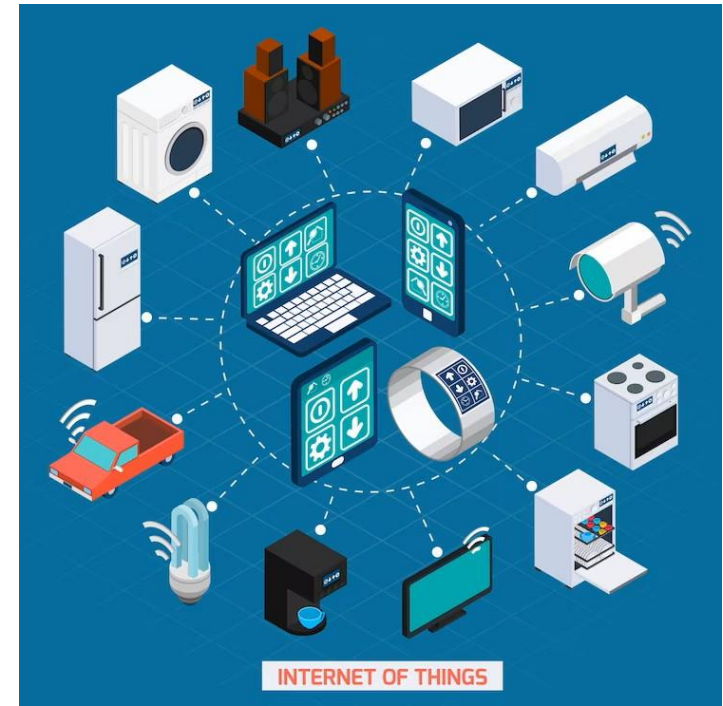


Chapter 01

IoT Network

An **IoT network** refers to a collection of devices such as sensors, gadgets, appliances, and software that communicate with each other and exchange information and data without the need for human intervention.

Through the power of cloud and edge computing businesses can now collect new insights from devices through IoT networks. This bridges the gap between the digital and physical world and allows organizations to monitor environmental, geolocation, and atmospheric conditions in real-time. When paired with automation, businesses can instantly react to changes in an environment, allowing for less downtime, better insights, and improved efficiency.



Chapter 01

IoT Platform

A multi-layer technology which is used to manage and automate the connected devices is known as the IoT platform. In other words, it is a service which helps you in bringing the physical objects online. This platform will provide you with the services to connect the devices for a machine to machine communication.

Build better and deploy faster with ThingWorx Foundation

Create robust industrial IoT solutions—faster and more easily than ever before. Harness deep functional capabilities and our robust IIoT partner ecosystem, to develop feature-rich IoT applications that maximize your return on investment.



Low-code IoT software platform for electronics manufacturers

You develop the hardware, Blynk covers the rest while you build, launch and scale your IoT business.



Internet of things > Solutions >

IoT platform

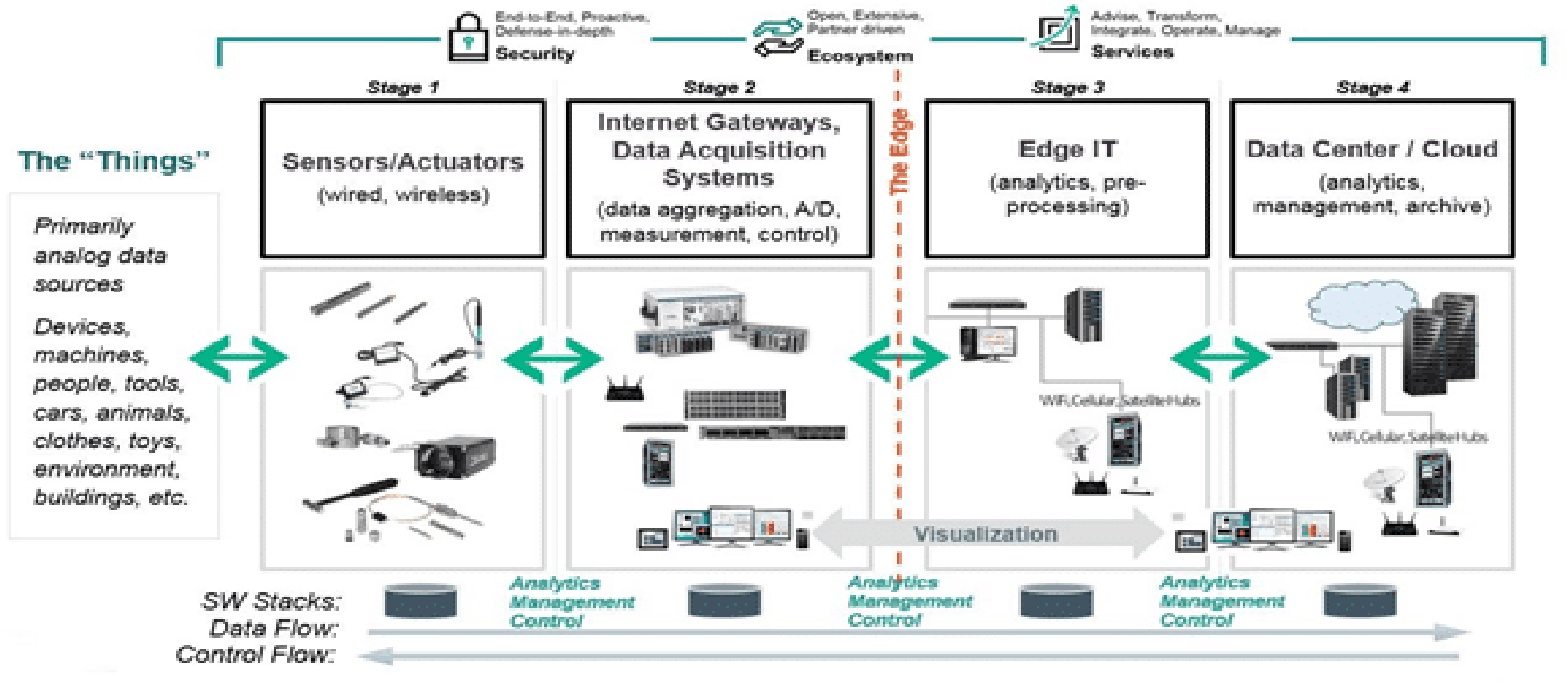
Take advantage of secure, globally distributed data and analytics to completely manage your IoT landscape



Chapter 01

IoT Architecture

The 4 Stage IoT Solutions Architecture



Smart devices

This is a device, like a television, security camera, or exercise equipment that has been given computing capabilities. It collects data from its environment, user inputs, or usage patterns and communicates data over the internet to and from its IoT application.

IoT application

An IoT application is a collection of services and software that integrates data received from various IoT devices. It uses machine learning or artificial intelligence (AI) technology to analyze this data and make informed decisions. These decisions are communicated back to the IoT device and the IoT dev, which intelligently to inputs.

A graphical user interface

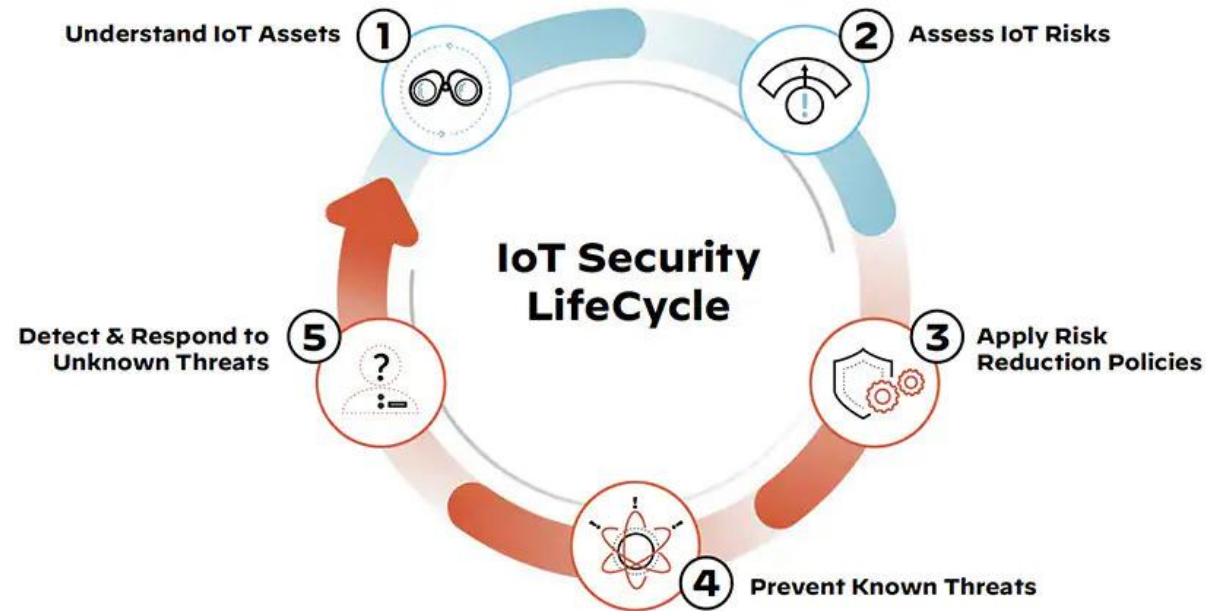
The IoT device or fleet of devices can be managed through a graphical user interface. Common examples include a mobile application or website that can be used to register and control smart devices.



Chapter 01

IoT Security

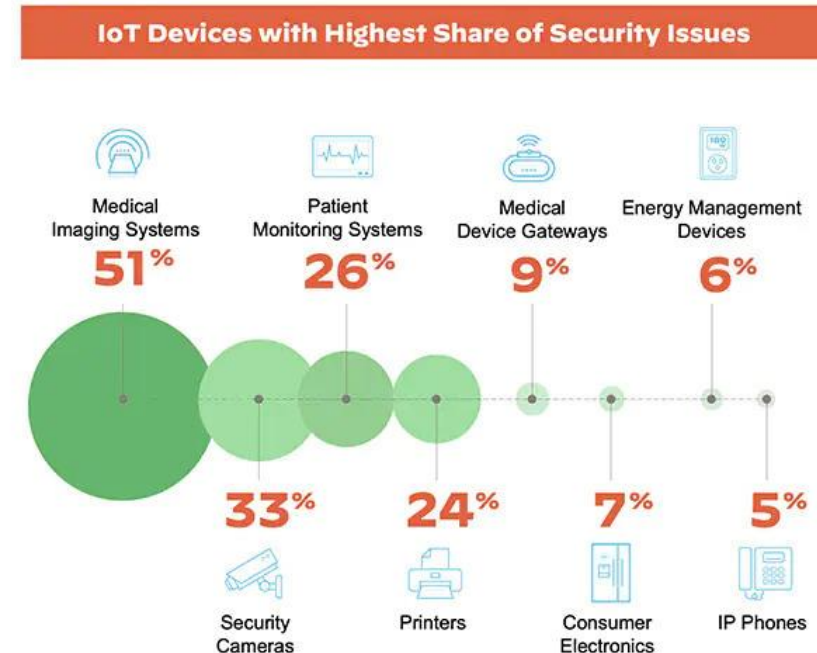
IoT security can be understood as a cybersecurity strategy and protection mechanism that safeguards against the possibility of cyberattacks which specifically target physical IoT devices that are connected to the network. Without robust security, any connected IoT device is vulnerable to breach, compromise and control by a bad actor to ultimately infiltrate, steal user data and bring down systems.



Chapter 01

IoT Security Challenges

Some of the most frequent attacks on IoT devices are exploits executed using techniques such as network scanning, remote code execution, command injection and others. Forty-one percent of attacks exploit device vulnerabilities, as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses. After compromising the first device, lateral movement is opened up to access other vulnerable devices and compromise them one by one.



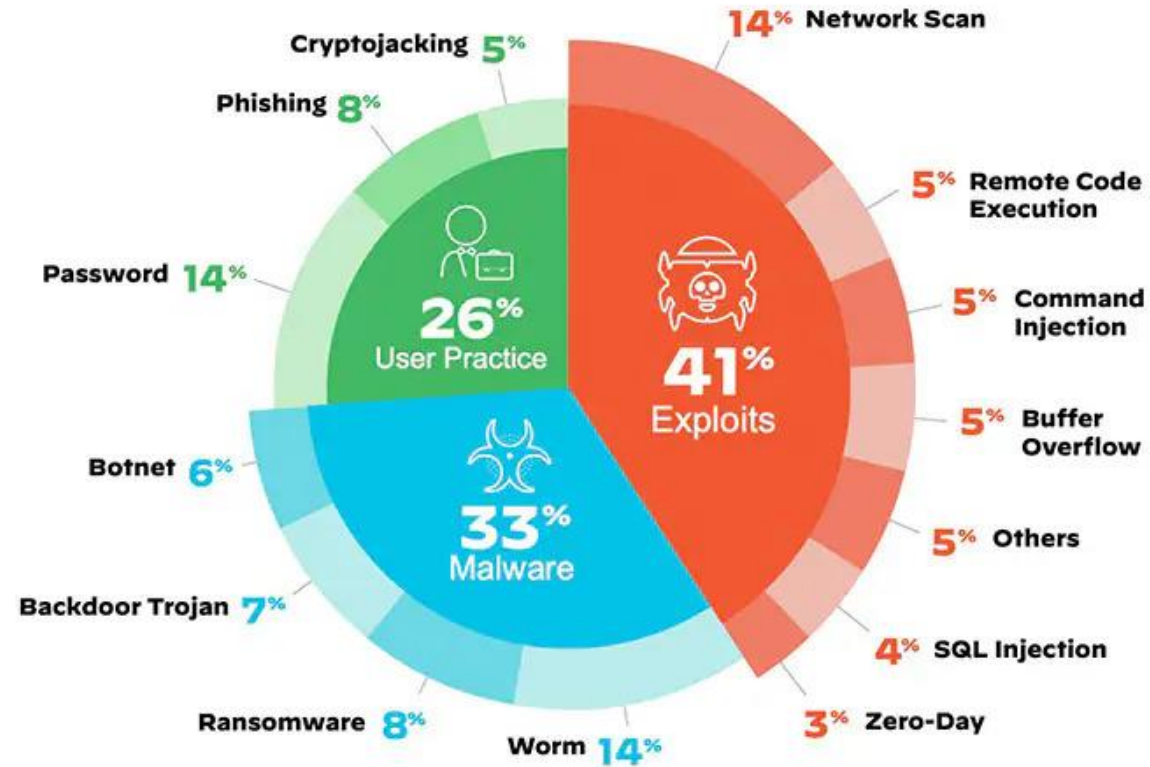
The Verkada hack

Verkada, a cloud-based video surveillance service, was hacked in March 2021. The attackers could access private information belonging to Verkada software clients and access live feeds of over 150,000 cameras mounted in factories, hospitals, schools, prisons, and other sites using legitimate admin account credentials found on the internet. Over 100 employees were later found to have "super admin" privileges, enabling them access to thousands of customer cameras, revealing the risks associated with over privileged users.



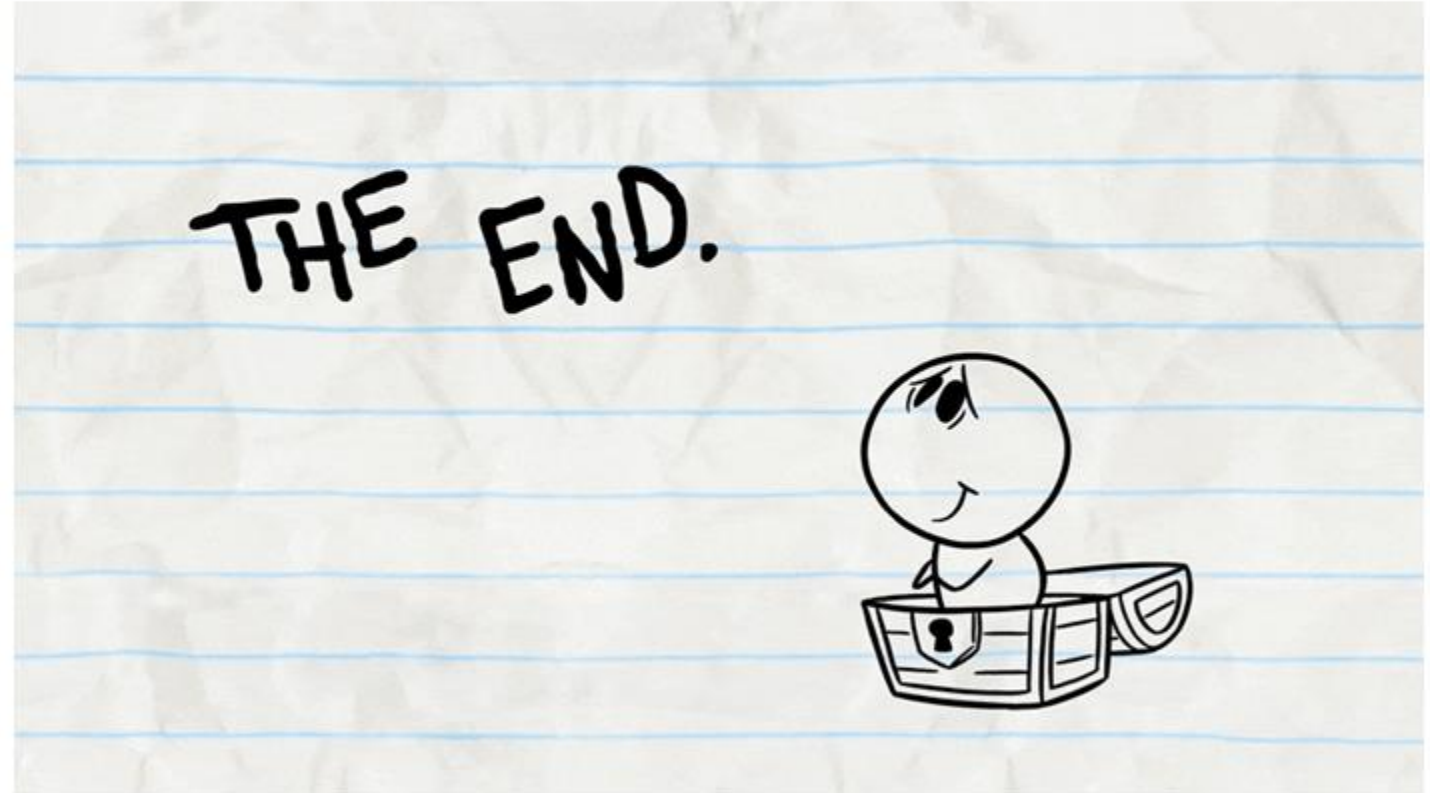
Chapter 01

Top Security Threats to IoT Devices



The End

Please feel free to contact me anytime if you have any questions



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY