CRYPTUS CYBER
SECURITY PVT. LTD.

Module Name:-

(IoT) Internet of Things

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects,

animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business.

How IoT works

An IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data.

The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed.

IoT can also make use of artificial intelligence (AI) and machine learning to aid in making data collecting processes easier and more dynamic.

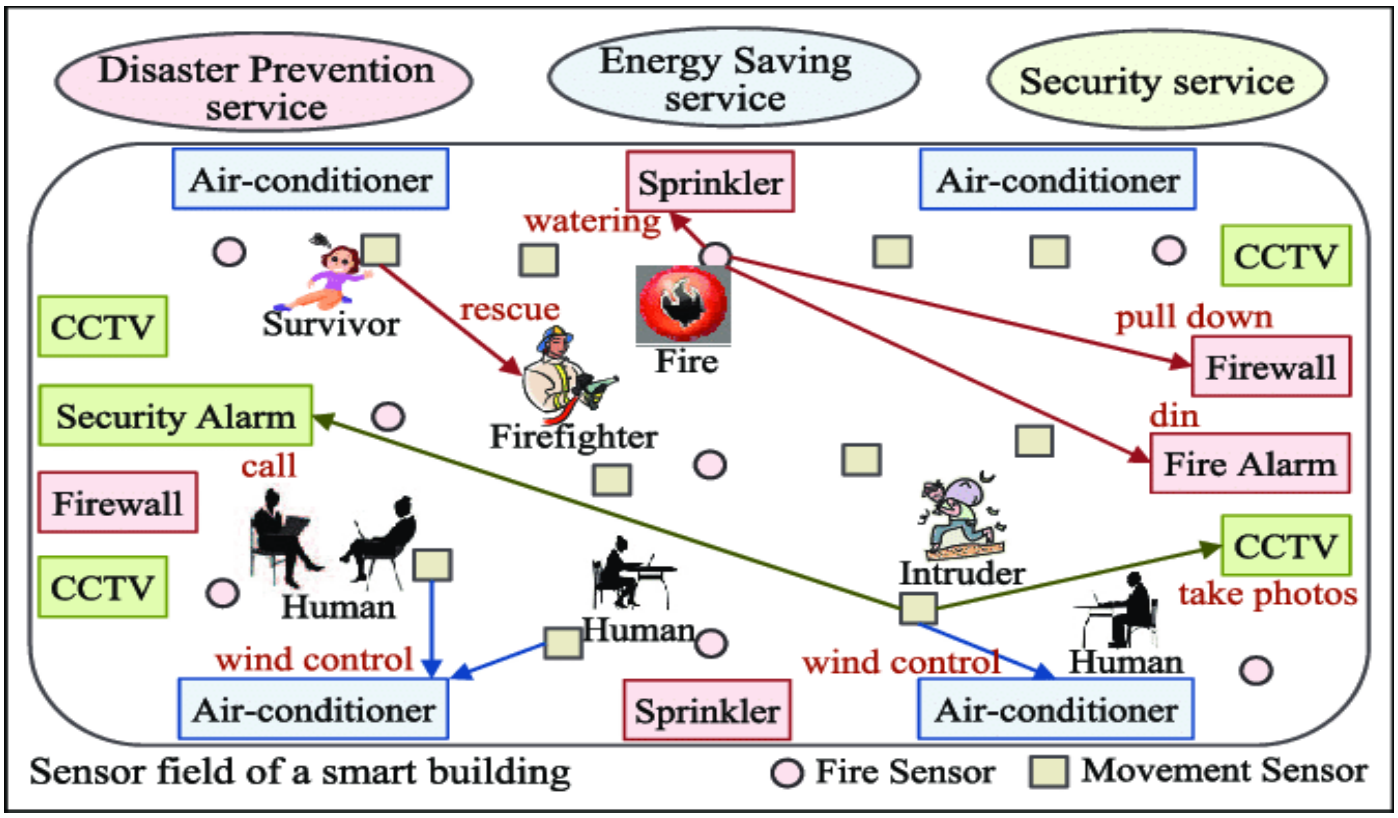
Why IoT is important

The internet of things helps people live and work smarter, as well as gain complete control over their lives. In addition to offering smart devices to automate homes, IoT is essential to business. IoT provides businesses with a real-time look into how their systems really work, delivering insights into everything from the performance of machines to supply chain and logistics operations.

IoT enables companies to automate processes and reduce labor costs. It also cuts down on waste and improves service delivery, making it less expensive to manufacture and deliver goods, as well as offering transparency into customer transactions.
As such, IoT is one of the most important technologies of everyday life, and it will continue to pick up steam as more businesses realize the potential of connected devices to keep them competitive.

IoT benefits to organizations

The internet of things offers several benefits to organizations. Some benefits are industry-specific, and some are applicable across multiple industries. Some of the common benefits of IoT enable businesses to:



monitor their overall business processes;
improve the customer experience (CX);
save time and money;
enhance employee productivity;
integrate and adapt business models;
make better business decisions; and
generate more revenue.
IoT encourages companies to rethink the ways they approach their businesses and gives them the tools to improve their business strategies.

Generally, IoT is most abundant in manufacturing, transportation and utility organizations, making use of sensors and other IoT devices; however, it has also found

use cases for organizations within the agriculture, infrastructure and home automation industries, leading some organizations toward digital transformation.

IoT can benefit farmers in agriculture by making their job easier. Sensors can collect data on rainfall, humidity, temperature and soil content, as well as other factors, that would help automate farming techniques.

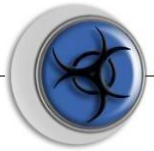
The ability to monitor operations surrounding infrastructure is also a factor that IoT can help with. Sensors, for example, could be used to monitor events or changes within structural buildings, bridges and other infrastructure. This brings benefits with it, such as cost saving, saved time, quality-of-life workflow changes and paperless workflow.

A home automation business can utilize IoT to monitor and manipulate mechanical and electrical systems in a building. On a broader scale, smart cities can help citizens reduce waste and energy consumption.

IoT touches every industry, including businesses within healthcare, finance, retail and manufacturing.

Pros and cons of IoT

Some of the advantages of IoT include the following:
ability to access information from anywhere at any time on any device;
improved communication between connected electronic devices;
transferring data packets over a connected network saving time and money; and
automating tasks helping to improve the quality of a business's services and reducing the need for human intervention.
Some disadvantages of IoT include the following:
As the number of connected devices increases and more information is shared between devices, the potential that a hacker could steal confidential information also increases.
Enterprises may eventually have to deal with massive numbers -- maybe even millions -- of IoT devices, and collecting and managing the data from all those devices will be challenging.
If there's a bug in the system, it's likely that every connected device will become corrupted.
Since there's no international standard of compatibility for IoT, it's difficult for devices from different manufacturers to communicate with each other.
IoT standards and frameworks
There are several emerging IoT standards, including the following:
IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) is an open standard defined by the Internet Engineering Task Force (IETF). The 6LoWPAN
ZigBee is a low-power, low-data rate wireless network used mainly in industrial settings. ZigBee is based on the Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 standard enables any low-power radio to communicate to the internet, including 804.15.4, Bluetooth Low Energy (BLE) and Z-Wave (for home automation.
standard.



The ZigBee Alliance created Dotdot, the universal language for IoT that enables smart objects to work securely on any network and understand each other.
LiteOS is a Unix-like operating system (OS) for wireless sensor networks. LiteOS supports smartphones, wearables, intelligent manufacturing applications, smart homes and the internet of vehicles (IoV). The OS also serves as a smart device development platform.
OneM2M is a machine-to-machine service layer that can be embedded in software and hardware to connect devices. The global standardization body, OneM2M, was created to develop reusable standards to enable IoT applications across different verticals to communicate.
Data Distribution Service (DDS) was developed by the Object Management Group (OMG) and is an IoT standard for real-time, scalable and high-performance M2M communication.
Advanced Message Queuing Protocol (AMQP) is an open source published standard for asynchronous messaging by wire. AMQP enables encrypted and interoperable messaging between organizations and applications. The protocol is used in client-server messaging and in IoT device management.
Constrained Application Protocol (CoAP) is a protocol designed by the IETF that specifies how low-power, compute-constrained devices can operate in the internet of things.
Long Range Wide Area Network (LoRaWAN) is a protocol for WANs designed to support huge networks, such as smart cities, with millions of low-power devices.
IoT frameworks include the following:

Amazon Web Services (AWS) IoT is a cloud computing platform for IoT released by Amazon. This framework is designed to enable smart devices to easily connect and securely interact with the AWS cloud and other connected devices.
Arm Mbed IoT is a platform to develop apps for IoT based on Arm microcontrollers. The goal of the Arm Mbed IoT platform is to provide a scalable, connected and secure environment for IoT devices by integrating Mbed tools and services.
Microsoft's Azure IoT Suite is a platform that consists of a set of services that enables users to interact with and receive data from their IoT devices, as well as perform various operations over data, such as multidimensional analysis, transformation and aggregation, and visualize those operations in a way that's suitable for business.
Google's Brillo/Weave is a platform for the rapid implementation of IoT applications. The platform consists of two main backbones: Brillo, an Android-based OS for the development of embedded low-power devices, and Weave, an IoT-oriented communication protocol that serves as the communication language between the device and the cloud.
Calvin is an open source IoT platform released by Ericsson designed for building and managing distributed applications that enable devices to talk to each other. Calvin includes a development framework for application developers, as well as a runtime environment for handling the running application.

Consumer and enterprise IoT applications

There are numerous real-world applications of the internet of things, ranging from consumer IoT and enterprise IoT to manufacturing and industrial IoT (IIoT). IoT applications span numerous verticals, including automotive, telecom and energy.

In the consumer segment, for example, smart homes that are equipped with smart thermostats, smart appliances and connected heating, lighting and electronic devices can be controlled remotely via computers and smartphones.

Wearable devices with sensors and software can collect and analyze user data, sending messages to other technologies about the users with the aim of making users' lives easier and more comfortable. Wearable devices are also used for public safety -- for example, improving first responders' response times during emergencies by providing optimized routes to a location or by tracking construction workers' or firefighters' vital signs at life-threatening sites.

In healthcare, IoT offers many benefits, including the ability to monitor patients more closely using an analysis of the data that's generated. Hospitals often use IoT systems to complete tasks such as inventory management for both pharmaceuticals and medical instruments.

Smart buildings can, for instance, reduce energy costs using sensors that detect how many occupants are in a room. The temperature can adjust automatically -- for example, turning the air conditioner on if sensors detect a conference room is full or turning the heat down if everyone in the office has gone home.

In agriculture, IoT-based smart farming systems can help monitor, for instance, light, temperature, humidity and soil moisture of crop fields using connected sensors. IoT is also instrumental in automating irrigation systems.

In a smart city, IoT sensors and deployments, such as smart streetlights and smart meters, can help alleviate traffic, conserve energy, monitor and address environmental concerns, and improve sanitation.

IoT security and privacy issues

The internet of things connects billions of devices to the internet and involves the use of billions of data points, all of which need to be secured. Due to its expanded attack surface, IoT security and IoT privacy are cited as major concerns.

In 2016, one of the most notorious recent IoT attacks was Mirai, a botnet that infiltrated domain name server provider Dyn and took down many websites for an extended period of time in one of the biggest distributed denial-of-service (DDoS) attacks ever seen. Attackers gained access to the network by exploiting poorly secured IoT devices.

Because IoT devices are closely connected, all a hacker has to do is exploit one vulnerability to manipulate all the data, rendering it unusable. Manufacturers that don't update their devices regularly -- or at all -- leave them vulnerable to cybercriminals.

Additionally, connected devices often ask users to input their personal information, including names, ages, addresses, phone numbers and even social media accounts -- information that's invaluable to hackers.

Hackers aren't the only threat to the internet of things; privacy is another major concern for IoT users. For instance, companies that make and distribute consumer IoT devices could use those devices to obtain and sell users' personal data.

Beyond leaking personal data, IoT poses a risk to critical infrastructure, including electricity, transportation and financial services.