

Chapter Seven

Other emerging technologies

Nanotechnology

Nanotechnology is science, engineering, and technology conducted at the nanoscale, which is about 1 to 100 nanometers. Nanoscience and nanotechnology are the study and application of extremely small things and can be used across all the other science fields, such as chemistry, biology, physics, materials science, and engineering.

It's hard to imagine just how small nanotechnology is. One nanometer is a billionth of a meter or 10^{-9} (ten the power of nine) of a meter. Here are a few illustrative examples:

- There are 25,400,000 nanometers in an inch
- A sheet of newspaper is about 100,000 nanometers thick
- On a comparative scale, if a marble were a nanometer, then one meter would be the size of the Earth

Nanoscience and nanotechnology involve the ability to see and to control individual atoms and molecules. Everything on Earth is made up of atoms—the food we eat, the clothes we wear, the buildings and houses we live in, and our own bodies.

Applications of nanotechnology

A. Medicine

B. Electronics

C. Food

D. Space

E. Agriculture

F. Vehicle manufacturers

G. Construction

H. Information and communication

Biotechnology

It is the broad area of biology involving living systems and organisms to develop or make products, or "any technological application that uses biological systems, living organisms, or derivatives thereof, to make or modify products or processes for specific use"

A. Agriculture

The use of **Biotechnology** in **Agriculture** is known as **Green Biotechnology**. The organisms formed after manipulation of genes is known as **Genetically Modified Organisms** such as Crops, Animals, Plants, Fungi, Bacteria, etc. Genetically modified crops are formed by the manipulation of **DNA** to introduce a new trait into the crops.

B. The use of biotechnology in medicine is known as **Medicinal Biotechnology**. This helps in the formation of genetically modified insulin known as humulin

C. Aquaculture Fisheries

It helps in improving the quality and quantity of fishes.

D. Production of Antibiotics

Plants are used to develop antibiotics for **Humans** as well as for **Animal** use. It helps in the production of antibiotics, vaccines and artificial hormones for hormone therapies.

E. Environment

Environmental biotechnology is used in waste

Autonomic computing (AC) is an approach to address the complexity and evolution problems in software systems. A software system that operates on its own or with a minimum of human interference according to a set of rules is called **autonomic**. The term autonomic derives from the human body's autonomic nervous system, which

Autonomic computing

is a self-managing computing model named after, and patterned on, the human body's autonomic nervous system. The goal of autonomic computing is to create systems that run themselves, capable of high-level functioning while keeping the system's complexity invisible to the user.

Autonomic systems/applications exhibit eight defining characteristics:

- ***Self Awareness***: An autonomic application/system “knows itself” and is aware of its state and its behaviors.
- ***Self Configuring***: An autonomic application/system should be able to configure and reconfigure itself under varying and unpredictable conditions.
- ***Self Optimizing***: An autonomic application/system should be able to detect suboptimal behaviors and optimize itself to improve its execution.
- ***Self-Healing***: An autonomic

- ▣ ***Self Protecting***: An autonomic application/system should be capable of detecting and protecting its resources from both internal and external attacks and maintaining overall system security and integrity.
- ▣ ***Context-Aware***: An autonomic application/system should be aware of its execution environment and be able to react to changes in the environment.
- ▣ ***Open***: An autonomic application/system must function in a heterogeneous world and should be portable across multiple hardware and software architectures. Consequently, it must be built on standard and open protocols and interfaces.
- ▣ ***Anticipatory***: An autonomic application/system should be able to anticipate to the extent possible, its needs and behaviors and those of its context, and be able to manage itself proactively.

It is an interdisciplinary scientific field that deals with how computers can be made to gain a high-level understanding of digital images or videos. From the perspective of engineering, it seeks to automate tasks that the human visual system can do.

Computer vision tasks include methods for acquiring, processing, analyzing and understanding digital images, and extraction of high-dimensional data from the real world in order to produce numerical or symbolic information, e.g. in the forms of decisions. nother way to define computer vision is through its applications. Computer vision is building algorithms that can understand the content of images and use it for other applications. computer vision is being used today in a wide variety of real-world applications, which include:

- ***Optical character recognition*** (OCR):
reading handwritten postal codes on letters and
automatic number plate recognition (ANPR)
 - ***Machine inspection***: looking for defects in
steel castings using X-ray vision
 - ***Retail***: object recognition for automated
checkout lanes
 - ***Medical imaging***: registering pre-operative
and intra-operative imagery or performing long-
term studies of people's brain morphology as
they age

□ ***Automotive safety:*** detecting unexpected obstacles such as pedestrians on the street, under conditions where active vision techniques such as radar or lidar do not work well

□ ***Surveillance:*** monitoring for intruders, analyzing highway traffic and monitoring pools for drowning victims.

□ ***Fingerprint recognition and biometrics:*** for automatic access authentication as well as forensic applications.

Embedded Systems

It is a controller with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is ***embedded*** as part of a complete device often including hardware and mechanical parts. Embedded systems control many devices in common use today. Ninety-eight percent of all microprocessors manufactured are used in embedded systems.

- A common standard class of dedicated processors is the digital signal processor (DSP).

Advantages of Embedded:

- ☐ Easily Customizable
- ☐ Low power consumption
- ☐ Low cost
- ☐ Enhanced performance

Disadvantages of Embedded systems

- ☐ High development effort
- ☐ Larger time to market

Sensor - It measures the physical quantity and converts it to an electrical signal which can be read by an observer or by any electronic instrument like an A2D converter. A sensor stores the measured quantity to the memory.

□ **A-D Converter** - An analog-to-digital converter converts the analog signal sent by the sensor into a digital signal.

□ **Processor & ASICs** - Processors process the data to measure the output and store it to the memory.

□ **D-A Converter** - A digital-to-analog converter converts the digital data fed by the processor to analog data.

□ **Actuator** - An actuator compares the output given by the D-A Converter to the actual (expected) output stored in it and stores the approved output

It is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. Cybersecurity is often confused with information security but it focuses on protecting computer systems from unauthorized access or being otherwise damaged or made inaccessible. Information security is a broader category that looks to protect all information assets, whether in hard copy or in digital form

Staff awareness training

Application security

Network security

Leadership commitment

Password management

Types of cybersecurity threats

Ransomware

Malware

Social engineering

Phishing

Benefits of cybersecurity

Benefits of utilizing cybersecurity include:

- Business protection against malware, ransomware, phishing, and social engineering.
- Protection for data and networks.
- Prevention of unauthorized users.
- Improves recovery time after a breach.
- Protection for end-users.
- Improved confidence in the product for both developers and customers

END