Chapter - 9 : Future Skills & Cyber Security

Introduction to FutureSkills :

FutureSkills in an industry utility to get Indi accelerated on a journey to build its skills and become the global hub for talent in emerging technologies. FutureSkills is the recourse for the IT-ITeS industry to enable discovery, continuous learning and deep skilling in 9 emerging technologies. There are 9 skills covered for this initiative and they are: Internet of Things, Big Data Analytics, cloud computing, virtual reality, Artificial Intelligence, Social& Mobile, Blockchain Technology, 3D printing, robotic Process Automation.

The futureSkills platform was launched by the Hon'ble Primce Minister of India, Shri Narendra Modi on 19th February, 2018 in the presence of senior industry leaders and government officials. FutureSkills subscription is currently open for NASSCOM member firms only.

Industrial Revolution

Industry 4.0 refers to a new industrial technology era that is transforming current systems, sensors, machines and workloads. The phrase 'fourth industrial revolution' was first introduced by Klaus Schwab in 2015 in the article in foreign affairs. First industrial Revolution started 18th century, second Industrial Revolution in 19th century, third Industrial Revolution started in mid 19th century and now we are facing Industry 4.0.

The fourth Industrial Revolution is fundamentally different from the previous three, which were characterized mainly by advances in technology. In this revolution, technologies have great potential to continue to connect billions of more people to the web, significantly improve the efficiency of business and organizations and help to regenerate the natural environment through better asset management.

Introduction to IOT:-

Certain devices can connect to the Internet so that you can share and receive information. Such devices include smartphones, tablets, PCs, and so on. Recently though, new devices have been introduced that can communicate with each other using the Internet and some other methods.

The full form of **IoT is "Internet of Things"**. The Internet of things is nothing but a network of various physical instruments or devices and other embedded items which with electronics, software, actuators over network connectivity.

The Internet of things is the extension of Internet connectivity into physical devices and everyday objects. Embedded with electronics, Internet connectivity, and other forms of hardware, these devices can communicate and interact with others over the Internet, and they can be remotely monitored and controlled.

More About of Internet of Things.

1. **The important components that exist in the Internet of Things are as follows**
    1. Hardware
    2. Software
    3. Verbal Exchange Infrastructure
2. **The elements of the Internet of Things are:**
    2. People
    3. Process
    4. Things
    5. Data

Big Data Analytics

The term "Big Data" may have been around for some time now, but there is still quite a lot of confusion about what it actually means. In truth, the concept is continually evolving and being reconsidered, as it remains the driving force behind many ongoing waves of digital transformation, including artificial intelligence, data science and the Internet of Things.

In big data analytics, we are presented with the data. The process of converting large amounts of unstructured raw data, retrieved from different sources to a data product useful for organizations forms the core of Big Data Analytics.

Characteristics of Big Data:-

1. Volume
2. Velocity
3. Variety
4. Veracity
5. Value

Cloud Computing:-

Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. Large clouds often have functions distributed over multiple locations, each location being a data center. Cloud computing relies on sharing of resources to achieve coherence and economies of scale. Cloud providers typically use a "pay-as-you-go" model, which can help in reducing capital expenses but may also lead to unexpected operating expenses for unaware users.

Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale. You typically pay only for cloud services you use, helping lower your operating costs, run your infrastructure more efficiently and scale as your business needs change.

Types of Cloud Computing:-

Public Cloud:-

Public clouds are owned and operated by a third-party cloud service providers, which deliver their computing resources like servers and storage over the Internet. **Microsoft Azure is an example of a public cloud.** With a public cloud, all hardware, software and other supporting infrastructure is owned and managed by the cloud provider. You access these services and manage your account using a web browser.

Amazon Elastic Compute Cloud (EC2), Microsoft Azure, IBM's Blue Cloud, Sun Cloud, and Google Cloud are examples of the public cloud.

Private Cloud:-

A private cloud refers to cloud computing resources used exclusively by a single business or organization. A private cloud can be physically located on the company's on-site datacenter. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.

HP Data Centers, Microsoft, Elastra-private cloud, and Ubuntu are the example of a private cloud.

Hybrid Cloud:-

Hybrid clouds combine public and private clouds, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, a hybrid cloud gives your business greater flexibility, more deployment options and helps optimize your existing infrastructure, security and compliance.

The best hybrid cloud provider companies are Amazon, Microsoft, Google, Cisco, and **NetApp**.

Types of Cloud Services/Service Models:-

It reference models on which the Cloud Computing is based. These can be categorized into three basic services as detailed below.

Infrastructure as a service (IaaS):-

The most basic category of cloud computing services. With IaaS, you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider on a pay-as-you-go basis.

Example:- Amazon EC2, Windows Azure, Rackspace, Google Compute Engine

Platform as a service (PaaS):-

Platform as a service refers to cloud computing services that supply an on-demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and databases needed for development.

Example:- AWS Elastic Beanstalk, Windows Azure, Heroku, force.com, Google App Engine, Apache Stratos.

Software as a service (SaaS):-

Software as a service is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet or PC.

Example:- Google Apps, Microsoft Office 365

Virtual Reality:-

Virtual reality is the term used to describe a three-dimensional, computer generated environment which can be explored and interacted with by a person. By simulating as many senses as possible, such as vision, hearing, touch, even smell, the computer is transformed into a portal to this artificial world. That person becomes part of this virtual world or is immersed within this environment and whilst there, is able to manipulate objects or perform a series of actions.

Virtual reality (VR) is an interactive computer-generated experience taking place within a simulated environment. VR technology allows sers to enter the virtual world and interact with virtual things. It is not limited to gaming, other application areas include enhancement of the education system, enablement of doctors to remotely handle surgeries, and contribution to industrial manufacturing processes and quality control among others.

Artificial Intelligence (AI):-

John McCarthy defined the term Artificial Intelligence in the year 1950. It is a concept that refers to a computer's ability to perform tasks and make decisions that require some level of human intelligence. AI is a part of our daily life. This technology is used in a wide range of day-to-day services. It reduces human effort.

There are several sectors that have already started the use of AI, like healthcare, automobiles, heavy industries, etc. many companies like Amazon, Facebook and Apple have identifies the value of this technology and are planning to invest more to advance their machine learning technology.

Social & Mobile:-

Mobile Devices and social media are part of Industry 4.0 because it is the major source of meaningful information for companies that it contains large amounts of data. This "digital transformation" can be challenging for the companies however, many companies are already started their journey to transformation since they provide interactive website, improved customer service and so on.

Popular Social Media Tools and Platforms

- Flickr
- YouTube & vimeo
- Snapchat
- Facebook
- Blogs

Blockchain Technology:-

Blockchain is the technology of Digital CryptoCurrency Bitcoin. It is a distributed database of records of all transactions that have been executed and shared among participating parties. Each transaction is verified by the majority of participants of the system. It contains every single record of each transaction. BitCoin is the most popular cryptocurrency example of the blockchain.

Block was invented by a person (or group of people) using the name "Satoshi Nakamoto" in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin.

3D Printing/Additive Manufacturing:-

3D printing is the automated process of building a three dimensional object by adding material rather than taking the material away. The process, also known as additive manufacturing, was first introduced in the late 1980s. it was first commercially used as a rapid prototyping method in the aerospace and automotive industries.

Robotics Process Automation:-

Robotic process automation (RPA) is a type of software that is used to do automation of fundamental tasks in software applications like how a human performs it. The software robot can be trained for a workflow/process with different steps & application.

RPA allows organizations to automate task just like a human being was doing them across application and systems. Robotic automation interacts with the existing IT architecture with no complex system integration required.

There are different types of tools in RPA

- Blue Prism
- UiPath
- Automation Anywhere
- Work Fusion
- Openspan

Cyber Security:-

Cyber security is the protection of Internet-connected systems, including hardware, software, and data. It is made up of two words one is cyber and other is security. Cyber is related to the technology which contains systems, network and programs or data. Whereas security related to the protection which includes systems security, network security and application and information security.

Need of Cyber Security:-

There are many types of cyber threats can attack your devices and networks, but they generally fall into three categories.

- Attacks on confidentiality
- Attacks on integrity
- Attacks on availability

Important Terminologies related to Cyber Security

Malware:-

It describes all forms of malicious software designed to damage a computer. Common forms include viruses, Trojans worms and ransomware.

Virus:-

A type of malware aimed to corrupt, erases or modify information on a computer before spreading to others. In more recent years, viruses like stuxnet have caused physical damage.

Ransomware:-

A form of malware that deliberately prevents you from accessing files on your computer- holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered. For example, WannaCry Ransomware

Trojan Horse:-

A piece of malware that often allows a hacker to gain remote access to a computer through a “back door”.

Worm:-

A piece of malware that can replicate itself in order to spread the infection to other connected computers.

Phishing:-

A technique used by hackers to obtain sensitive information.

Antivirus Software:-

It is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, Trojans adware, and more.

Spam:-

It refers to unsolicited commercial email (UCE) or Unsolicited Bulk Email (UBE).

Spyware:-

It is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information. Spyware is classified as a type of malware-malicious software designed to gain access to or damage your computer, often without your knowledge.

Securing PC:-

If you find yourself using a virus-ridden computer, you could have your personal data stolen and sold on. On top of that, your PC or laptop will run slower than it should, sometimes making it entirely unusable. It's now more important than ever to keep your computer protected. But what's the best way to stay secure? Having up-to-date virus protection helps, but there are other ways to guard your tech.

- Set up two-step verification
- Schedule your virus scans
- Only install software from trusted sources
- Be wary of Google Chrome extensions
- Know how to spot a phishing scam
- Only use trusted sites when providing your personal information
- Don't open email attachments or click links in emails from unknown sources
- Always keep your devices updated
- Back up your files regularly
- Enable your firewall
- Adjust your browser settings
- Install Antivirus & spyware software
- Password protects your software and locks your device
- Encrypt your data
- Use a VPN

Securing Smart Phone:-

Phone security is the practice of defending mobile devices against a wide range of cyber attack vectors that threaten user's privacy, network login credentials, finances, and safety.

There are following ways to secure your mobile:-

- Establish a clear mobile usage policy
- Segment data and apps on enterprise devices
- Encrypt and minimize visibility into devices that have access to the company network
- Install security software on mobile devices
- Secure Payment Transactions
- Implement ATS (App Transport Security)
- Set a passcode
- Check your phone bill
- Download from trusted sources
- Backup and secure your data
- Understand app permission before accepting them
- Wipe data on your old phone before you donate, resell or recycle it
- Make sure you have a security app

Hacker:-

A computer hacker is a computer expert who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means.

There are three main types of hackers

Black hat hacker:-

Black hat hackers are responsible for all that is wrong with hacking. These guys break into systems purely with negative intentions. From stealing credit card information to altering public databases, a black hat hacker looks to gain fame or monetary benefits from exploiting the loopholes in internet frameworks.

White hat hacker:-

The white hat hacker is a good guy, as ironic as it may sound. White hackers, white hat hackers or ethical hackers are the people who test existing internet infrastructures to research loopholes in the system.

Grey hat hacker:-

A grey hat hacker usually has mixed intentions. As the color code implies, this hacker type does not have the good intentions of a white hat hacker, nor does he have the ill intentions of a black hacker. A grey hat would break into systems but never for his own benefit.