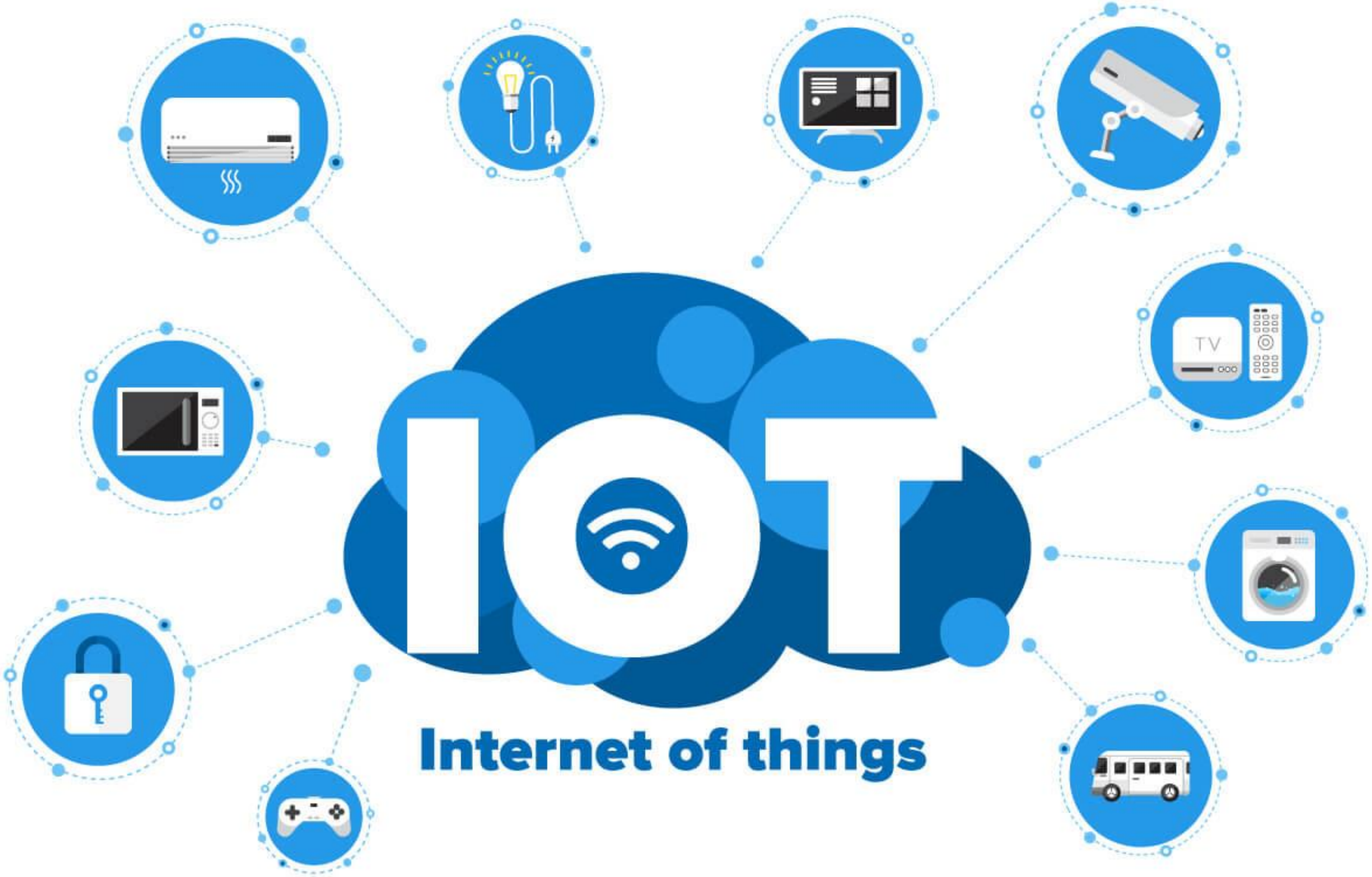
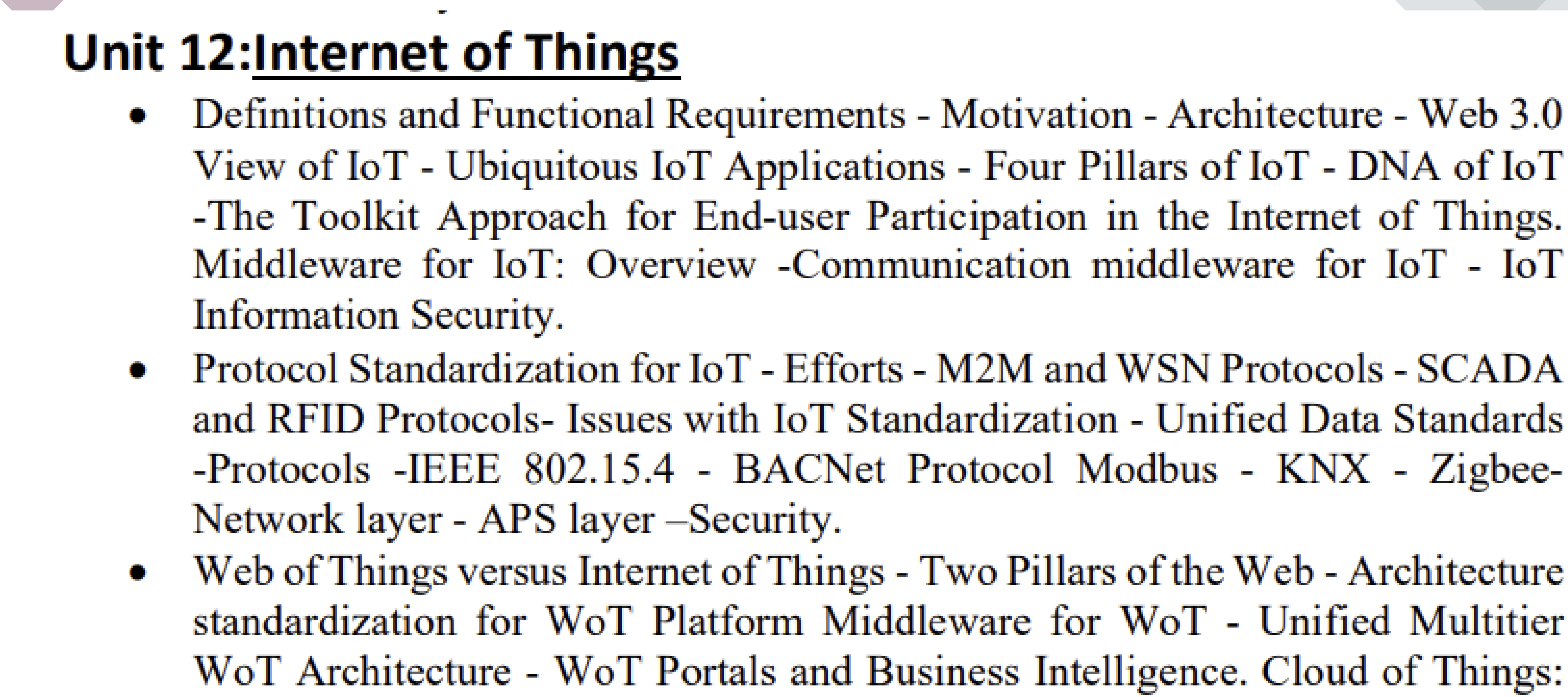
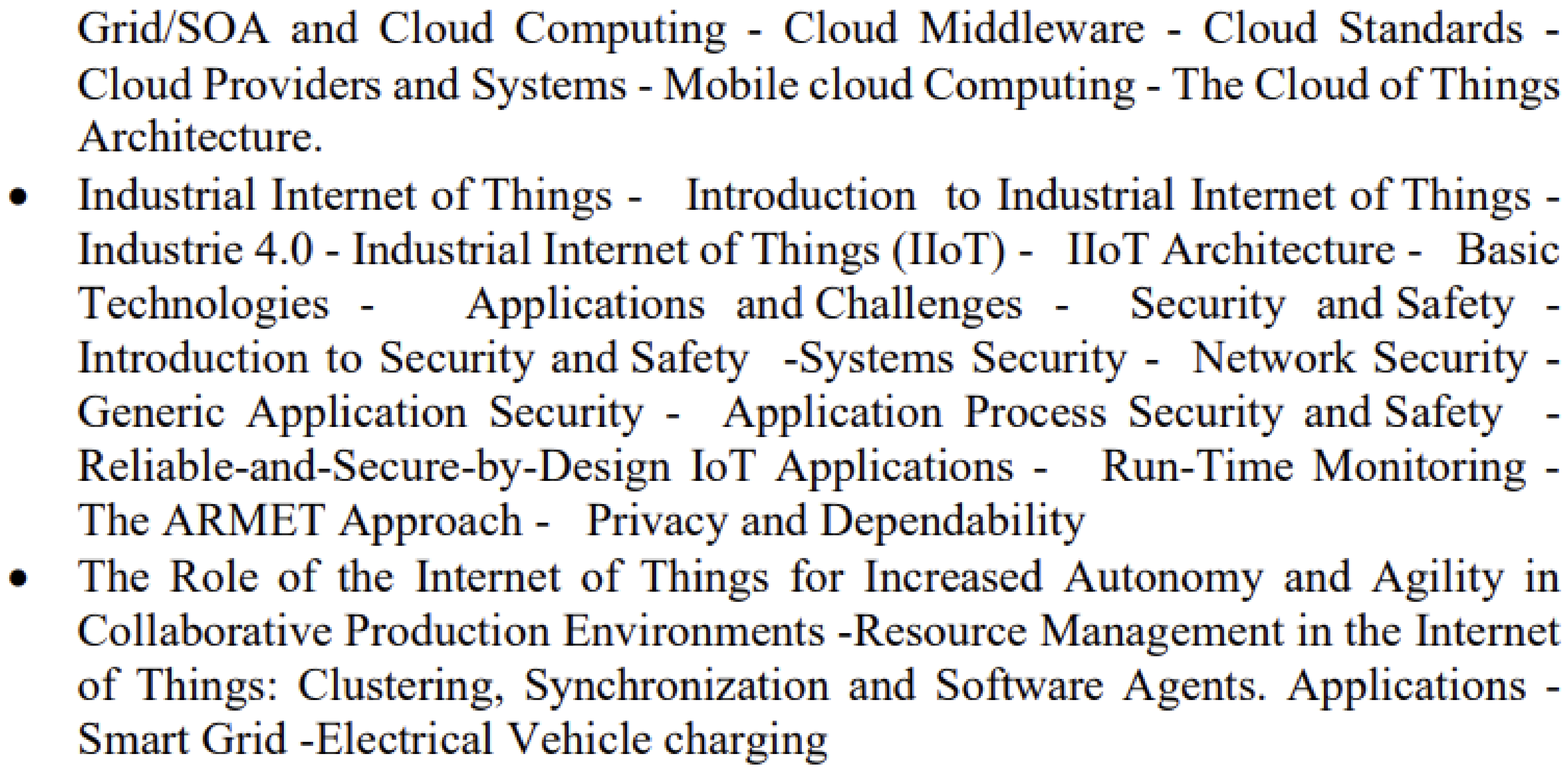

IOT
Internet of things
TV



Unit 12: Internet of Things

- Definitions and Functional Requirements - Motivation - Architecture - Web 3.0 View of IoT - Ubiquitous IoT Applications - Four Pillars of IoT - DNA of IoT -The Toolkit Approach for End-user Participation in the Internet of Things. Middleware for IoT: Overview -Communication middleware for IoT - IoT Information Security.
- Protocol Standardization for IoT - Efforts - M2M and WSN Protocols - SCADA and RFID Protocols- Issues with IoT Standardization - Unified Data Standards -Protocols -IEEE 802.15.4 - BACNet Protocol Modbus - KNX - Zigbee-Network layer - APS layer –Security.
- Web of Things versus Internet of Things - Two Pillars of the Web - Architecture standardization for WoT Platform Middleware for WoT - Unified Multitier WoT Architecture - WoT Portals and Business Intelligence. Cloud of Things:



Grid/SOA and Cloud Computing - Cloud Middleware - Cloud Standards - Cloud Providers and Systems - Mobile cloud Computing - The Cloud of Things Architecture.

- Industrial Internet of Things - Introduction to Industrial Internet of Things - Industrie 4.0 - Industrial Internet of Things (IIoT) - IIoT Architecture - Basic Technologies - Applications and Challenges - Security and Safety - Introduction to Security and Safety -Systems Security - Network Security - Generic Application Security - Application Process Security and Safety - Reliable-and-Secure-by-Design IoT Applications - Run-Time Monitoring - The ARMET Approach - Privacy and Dependability
- The Role of the Internet of Things for Increased Autonomy and Agility in Collaborative Production Environments -Resource Management in the Internet of Things: Clustering, Synchronization and Software Agents. Applications - Smart Grid -Electrical Vehicle charging

✓ Introduction to Internet of Things (IoT)

- ✓ IoT stands for Internet of Things. It refers to the interconnectedness of physical devices, such as appliances and vehicles, that are embedded with software, sensors, and connectivity which enables these objects to connect and exchange data. This technology allows for the collection and sharing of data from a vast network of devices, creating opportunities for more efficient and automated systems.

TA TEACHERS ADDA BY TARGET ABHI 7877719287

✓ Introduction to Internet of Things (IoT)

✓ Internet of Things (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment. In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives. Advancements in medicine, power, gene therapies, agriculture, smart cities, and smart homes are just a few of the categorical examples where IoT is strongly established.

TEACHERS ADDA BY TARGET ABHI 7877719287

✓ Introduction to the Internet of Things (IoT)

✓ IOT is a system of interrelated things, computing devices, mechanical and digital machines, objects, animals, or people that are provided with unique identifiers. And the ability to transfer the data over a network requiring human-to-human or human-to-computer interaction

- 1982 – Vending machine: The first glimpse of IoT emerged as a vending machine at Carnegie Mellon University was connected to the internet to report its inventory and status, paving the way for remote monitoring.
- 1990 – Toaster: Early IoT innovation saw a toaster connected to the internet, allowing users to control it remotely, foreshadowing the convenience of smart home devices.
- 1999 – IoT Coined (Kevin Ashton): Kevin Ashton coined the term “Internet of Things” to describe the interconnected network of devices communicating and sharing data, laying the foundation for a new era of connectivity.
- 2000 – LG Smart Fridge: The LG Smart Fridge marked a breakthrough, enabling users to check and manage refrigerator contents remotely, showcasing the potential of IoT in daily life.
- 2004 – Smart Watch: The advent of smartwatches introduced IoT to the wearable tech realm, offering fitness tracking and notifications on-the-go.
- 2007 – Smart iPhone: Apple’s iPhone became a game-changer, integrating IoT capabilities with apps that connected users to a myriad of services and devices, transforming smartphones into hubs.
- 2009 – Car Testing: IoT entered the automotive industry, enhancing vehicles with sensors for real-time diagnostics, performance monitoring, and remote testing.
- 2011 – Smart TV: The introduction of Smart TVs brought IoT to the living room, enabling internet connectivity for streaming, app usage, and interactive content.
- 2013 – Google Lens: Google Lens showcased IoT’s potential in image recognition, allowing smartphones to provide information about objects in the physical world.
- 2014 – Echo: Amazon’s Echo, equipped with the virtual assistant Alexa, demonstrated the power of voice-activated IoT, making smart homes more intuitive and responsive.
- 2015 – Tesla Autopilot: Tesla’s Autopilot system exemplified IoT in automobiles, introducing semi-autonomous driving capabilities through interconnected sensors and software.

✓ Four Key Components of IOT

✓ Device or sensor

✓ Connectivity

✓ Data processing

✓ Interface

TEACHERS ADDA BY TARGET ABHI 7877719287

□ **Control Units:** It is a unit of small computer on a single integrated circuit containing microprocessor or processing core, memory and programmable input/output devices/peripherals. It is responsible for major processing work of IoT devices and all logical operations are carried out here.

□ **Cloud computing:** Data collected through IoT devices is massive, and this data has to be stored on a reliable storage server. This is where cloud computing comes into play. The data is processed and learned, giving more room for us to discover where things like electrical faults/errors are within the system

TEACHERS ADDA BY TARGET ABHI 7877719287

- **Availability of big data:** We know that IoT relies heavily on sensors, especially in real-time. As these electronic devices spread throughout every field, their usage is going to trigger a massive flux of big data.

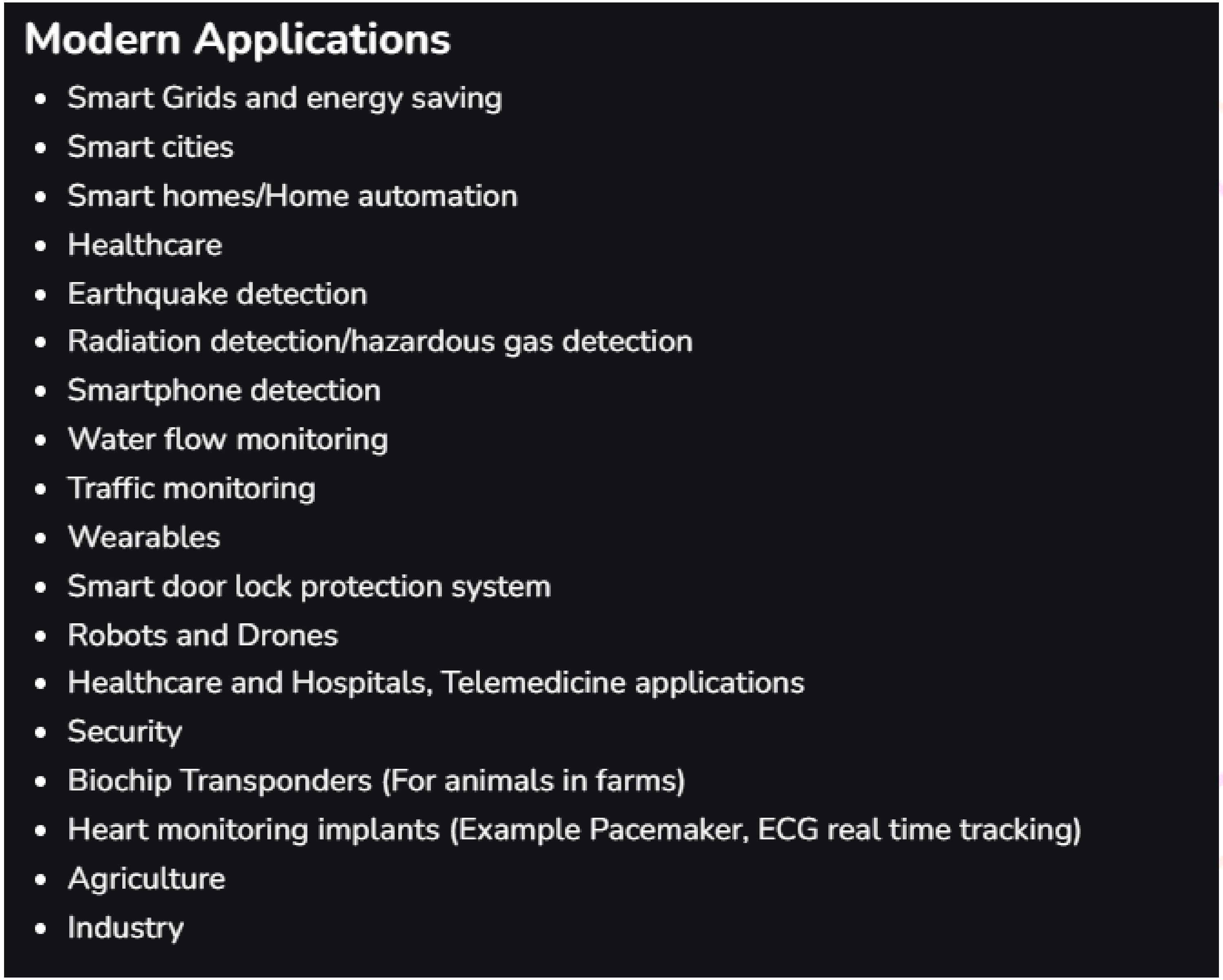
- **Networking connection:** In order to communicate, internet connectivity is a must, where each physical object is represented by an IP address. However, there are only a limited number of addresses available according to the IP naming. Due to the growing number of devices, this naming system will not be feasible anymore. Therefore, researchers are looking for another alternative naming system to represent each physical object.

TEACHERS ADDA BY TARGET ABHI 7877719287

Characteristics of IoT

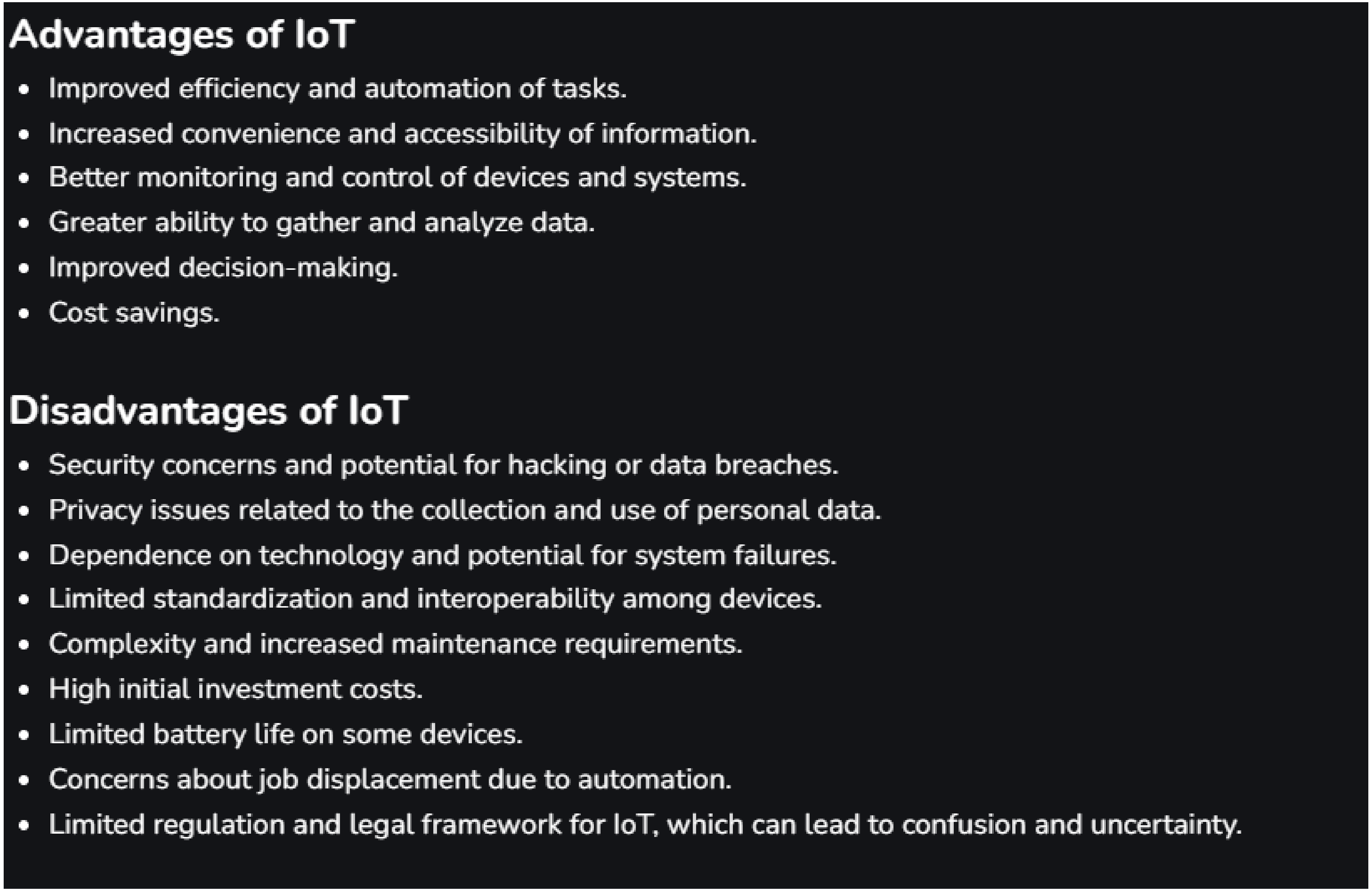
- ✓ Massively scalable and efficient
- ✓ IP-based addressing will no longer be suitable in the upcoming future.
- ✓ An abundance of physical objects is present that do not use IP, so IoT is made possible.
- ✓ Devices typically consume less power. When not in use, they should be automatically programmed to sleep.
- ✓ A device that is connected to another device right now may not be connected in another instant of time.
- ✓ Intermittent connectivity – IoT devices aren’t always connected. In order to save bandwidth and battery consumption, devices will be powered off periodically when not in use. Otherwise, connections might turn unreliable and thus prove to be inefficient.

TEACHERS ADDA BY TARGET ABHI 7877719287



Modern Applications

- Smart Grids and energy saving
- Smart cities
- Smart homes/Home automation
- Healthcare
- Earthquake detection
- Radiation detection/hazardous gas detection
- Smartphone detection
- Water flow monitoring
- Traffic monitoring
- Wearables
- Smart door lock protection system
- Robots and Drones
- Healthcare and Hospitals, Telemedicine applications
- Security
- Biochip Transponders (For animals in farms)
- Heart monitoring implants (Example Pacemaker, ECG real time tracking)
- Agriculture
- Industry



Advantages of IoT

- Improved efficiency and automation of tasks.
- Increased convenience and accessibility of information.
- Better monitoring and control of devices and systems.
- Greater ability to gather and analyze data.
- Improved decision-making.
- Cost savings.

Disadvantages of IoT

- Security concerns and potential for hacking or data breaches.
- Privacy issues related to the collection and use of personal data.
- Dependence on technology and potential for system failures.
- Limited standardization and interoperability among devices.
- Complexity and increased maintenance requirements.
- High initial investment costs.
- Limited battery life on some devices.
- Concerns about job displacement due to automation.
- Limited regulation and legal framework for IoT, which can lead to confusion and uncertainty.

Standardizing the IoT

Smart objects produce large volumes of data. This data needs to be managed, processed, transferred and stored securely. Standardization is key to achieving universally accepted specifications and protocols for true interoperability between devices and applications.

The use of standards:

- ✓ ensures interoperable and cost-effective solutions
- ✓ opens up opportunities in new areas
- ✓ allows the market to reach its full potential
- ✓ The more things are connected, the greater the security risk. So, security standards are also needed to protect the individuals, businesses and governments which will use the IoT.

TEACHERS ADDA BY TARGET ABHI 7877719287

Standardizing the IoT

Smart Machine-to-Machine (M2M) communications

ETSI is one of the founding partners in oneM2M, the global standards initiative that covers requirements, architecture, Application Programming Interface (API) specifications, security solutions and interoperability for M2M and IoT technologies.

TEACHERS ADDA BY TARGET ABHI 7877719287

Standardizing the IoT

Wireless Sensor Network (WSN):

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System.
Base Station in a WSN System is connected through the Internet to share data.

Components of WSN:

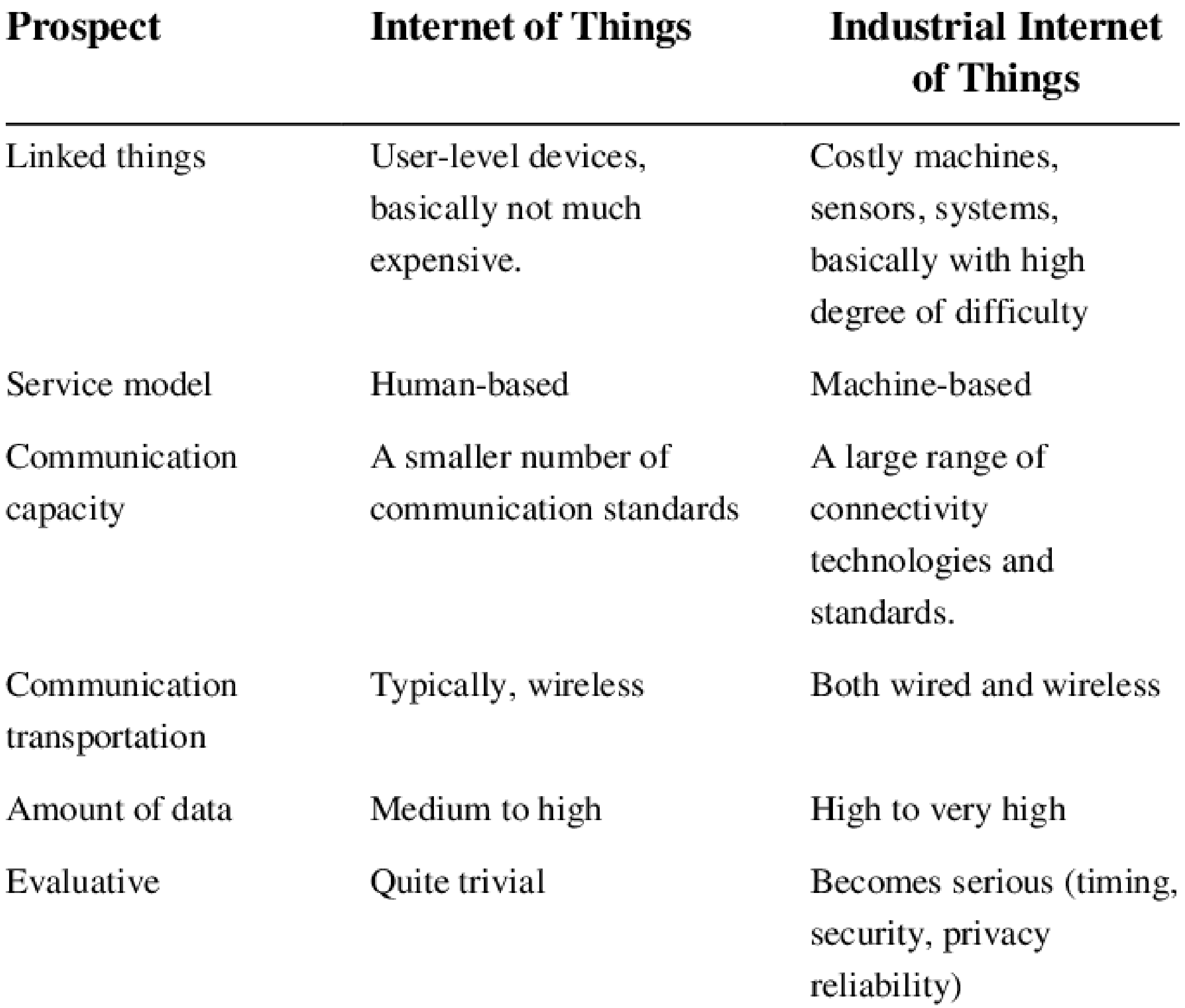
- Sensors:
- Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.
- Radio Nodes:
- It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.
- WLAN Access Point:
- It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.
- Evaluation Software:
- The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

❖ Industrial Internet of Things (IIoT)

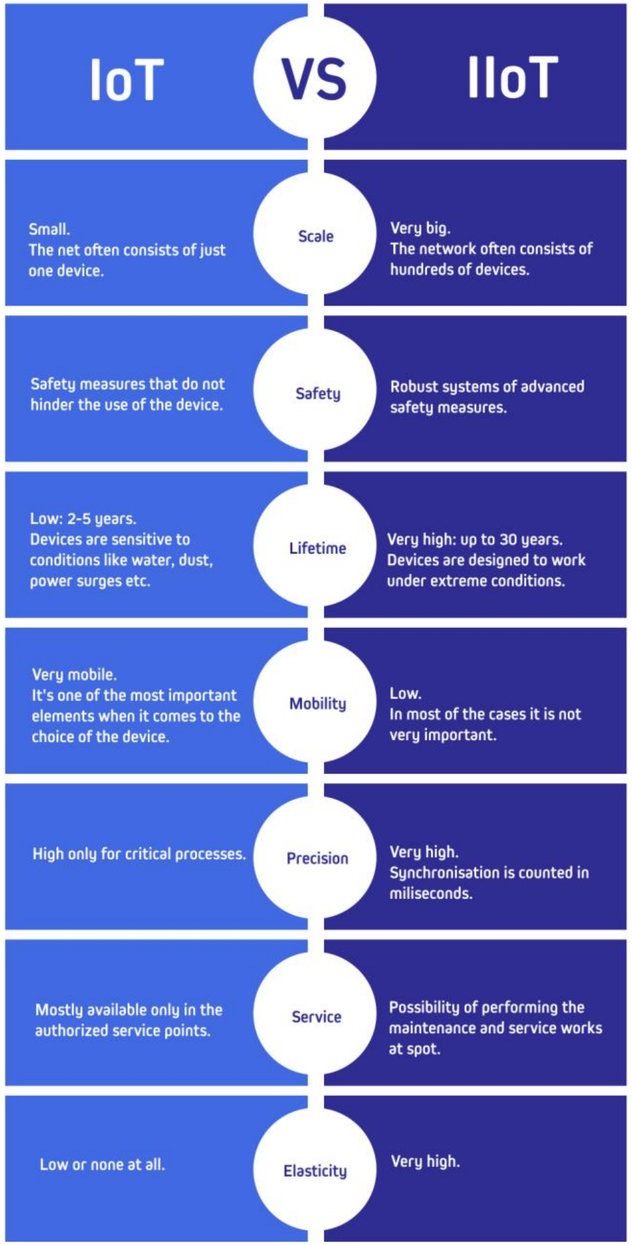
- As the name suggests, these are IoT devices used in the industry.
- The large-scale implementation of IoT devices requires knowledge of many issues in the field of, among others: IT security, robotics, inter-machine communication, automation, the Cloud services, artificial intelligence (AI), machine learning, and Big Data.
- Despite the high level of complexity, proper IIoT implementation has a number of benefits, e.g. more accurate monitoring of quality and production rate, resource and supply chain management, and improved workplace safety.

TEACHERS ADDA BY TARGET ABHI 7877719287

Iot vs IIoT



Prospect	Internet of Things	Industrial Internet of Things
Linked things	User-level devices, basically not much expensive.	Costly machines, sensors, systems, basically with high degree of difficulty
Service model	Human-based	Machine-based
Communication capacity	A smaller number of communication standards	A large range of connectivity technologies and standards.
Communication transportation	Typically, wireless	Both wired and wireless
Amount of data	Medium to high	High to very high
Evaluative	Quite trivial	Becomes serious (timing, security, privacy reliability)



IoT	VS	IIoT
Small. The net often consists of just one device.	Scale	Very big. The network often consists of hundreds of devices.
Safety measures that do not hinder the use of the device.	Safety	Robust systems of advanced safety measures.
Low: 2-5 years. Devices are sensitive to conditions like water, dust, power surges etc.	Lifetime	Very high: up to 30 years. Devices are designed to work under extreme conditions.
Very mobile. It's one of the most important elements when it comes to the choice of the device.	Mobility	Low. In most of the cases it is not very important.
High only for critical processes.	Precision	Very high. Synchronisation is counted in miliseconds.
Mostly available only in the authorized service points.	Service	Possibility of performing the maintenance and service works at spot.
Low or none at all.	Elasticity	Very high.

Network Security

नेटवर्क सुरक्षा

Network Security

Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems.

Different Types Of Network Security

1. **Access Control.**

This refers to controlling which users have access to the network or especially sensitive sections of the network.

Different Types Of Network Security

2. Antivirus and anti-malware software

- Malware, or "malicious software," is a common form of cyberattack that comes in many different shapes and sizes.

- Some variations work quickly to delete files or corrupt data, while others can lie dormant for long periods of time and quietly allow hackers a back door into your systems.

Different Types Of Network Security

3. Email security :

- Email is an especially important factor to consider when implementing networking security tools.

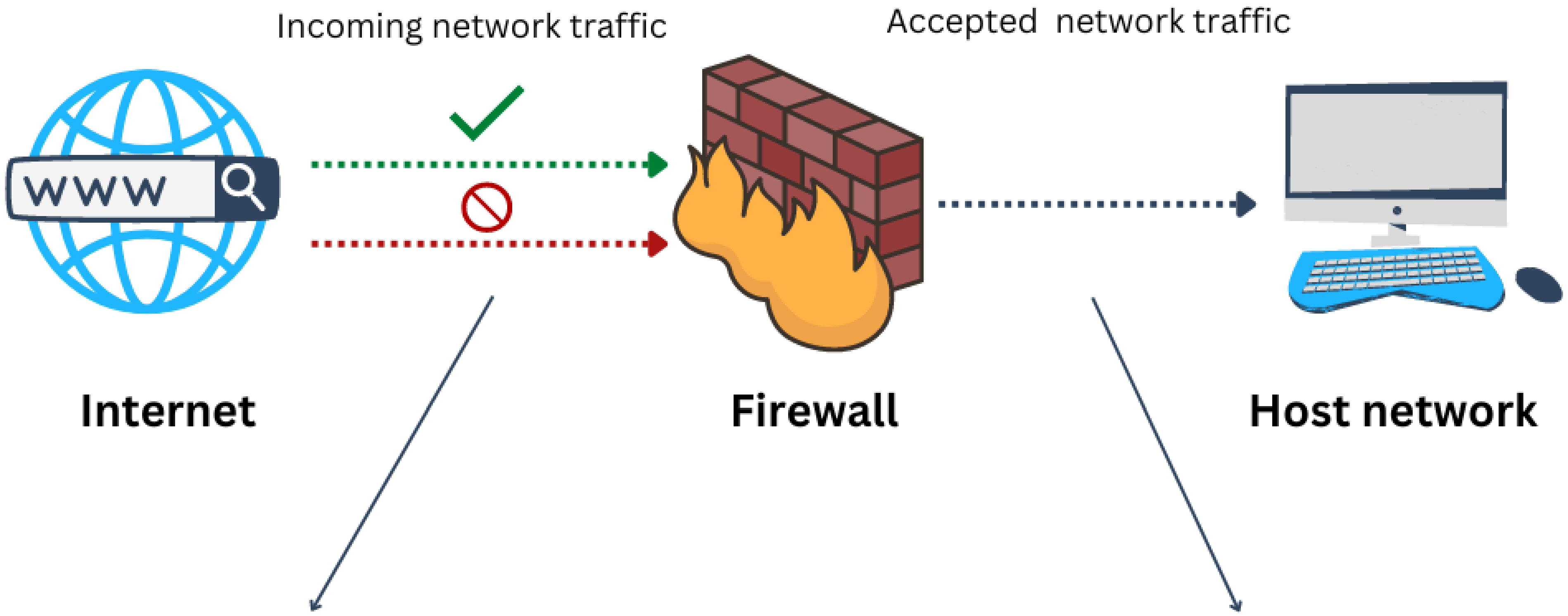
- Thousands threat like scams, phishing, malware, and suspicious links, can be attached to or incorporated into emails.

4. Firewalls :

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

- Firewalls have been a first line of defense in network security. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

- A firewall can be hardware, software, or both.



Incoming network traffic

Accepted network traffic

Internet

Firewall

Host network

The firewall controls and filters incoming network traffic to decide whether it should be accepted or restricted.

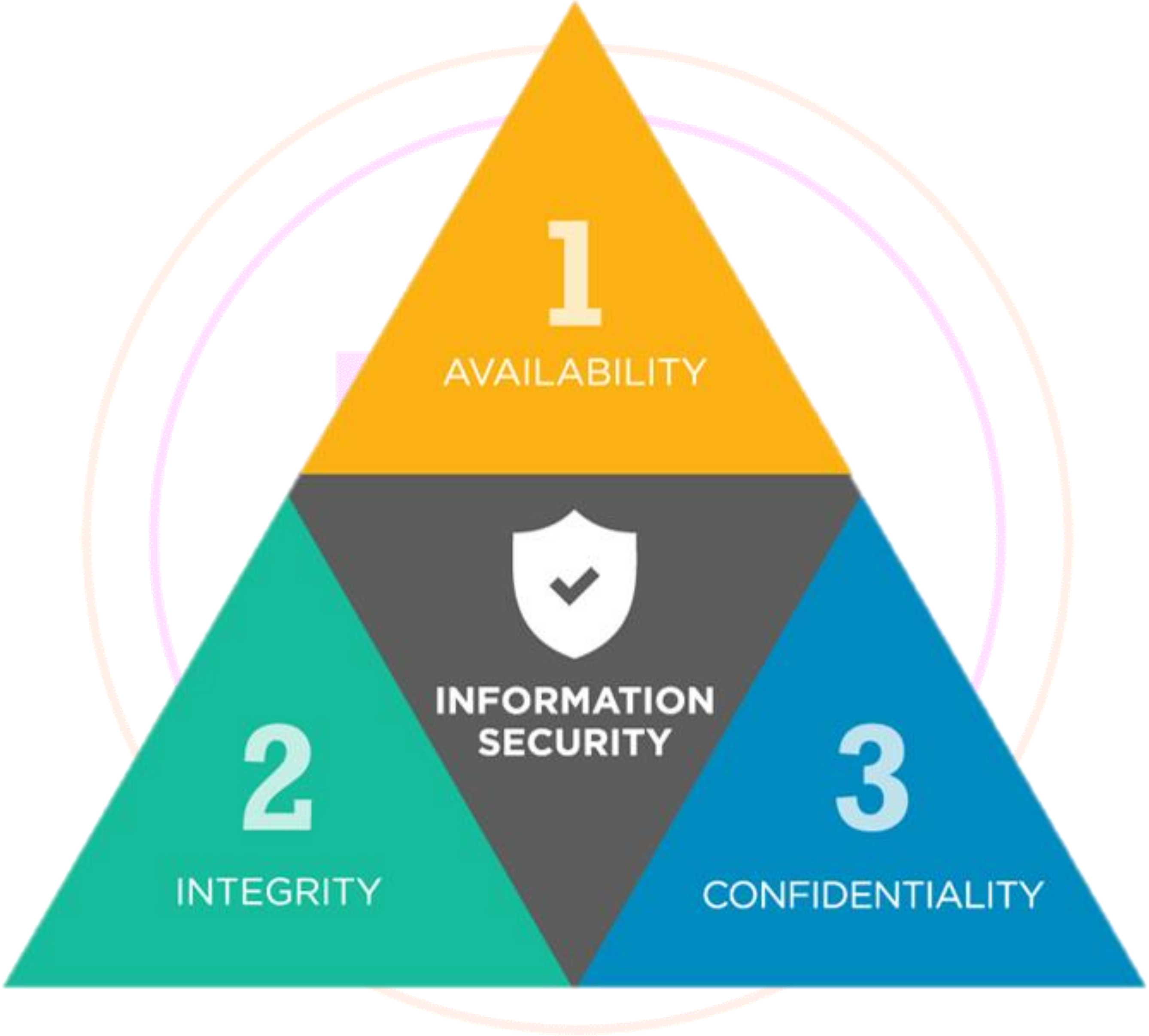
The firewall forwards accepted network traffic to the host machine and blocks suspicious activities based on predefined rules.

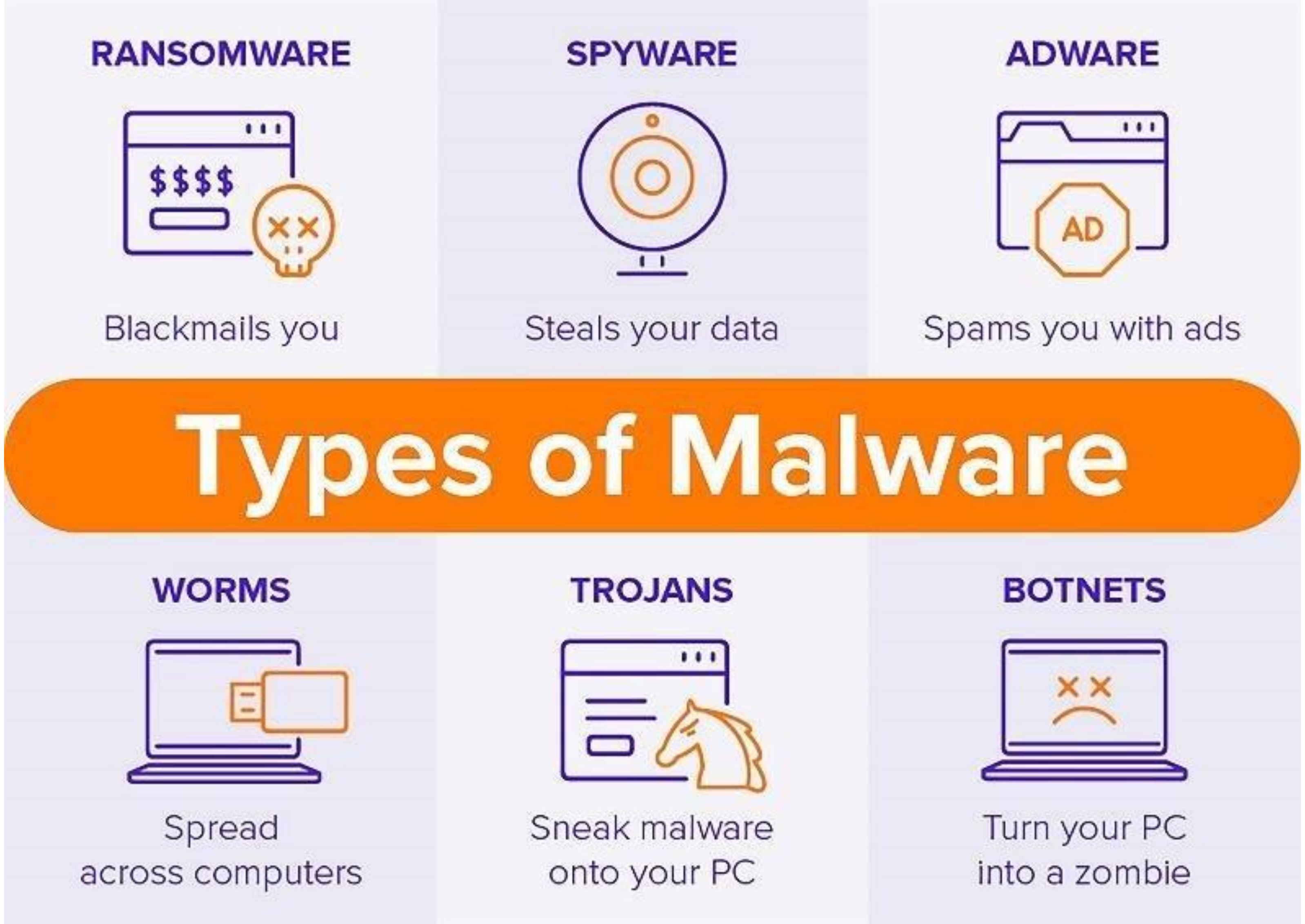
Different Types Of Network Security

5. Web security :

- Web security software serves a few purposes. it limits internet access for employees, with the intention of preventing them from accessing sites that could contain malware.

- It also blocks other web-based threats and works to protect a customer’s web gateway.


1
AVAILABILITY
INFORMATION SECURITY
2
INTEGRITY
3
CONFIDENTIALITY



Types of Malware

RANSOMWARE

Blackmails you

SPYWARE

Steals your data

ADWARE

Spams you with ads

WORMS

Spread across computers

TROJANS

Sneak malware onto your PC

BOTNETS

Turn your PC into a zombie

Brute force

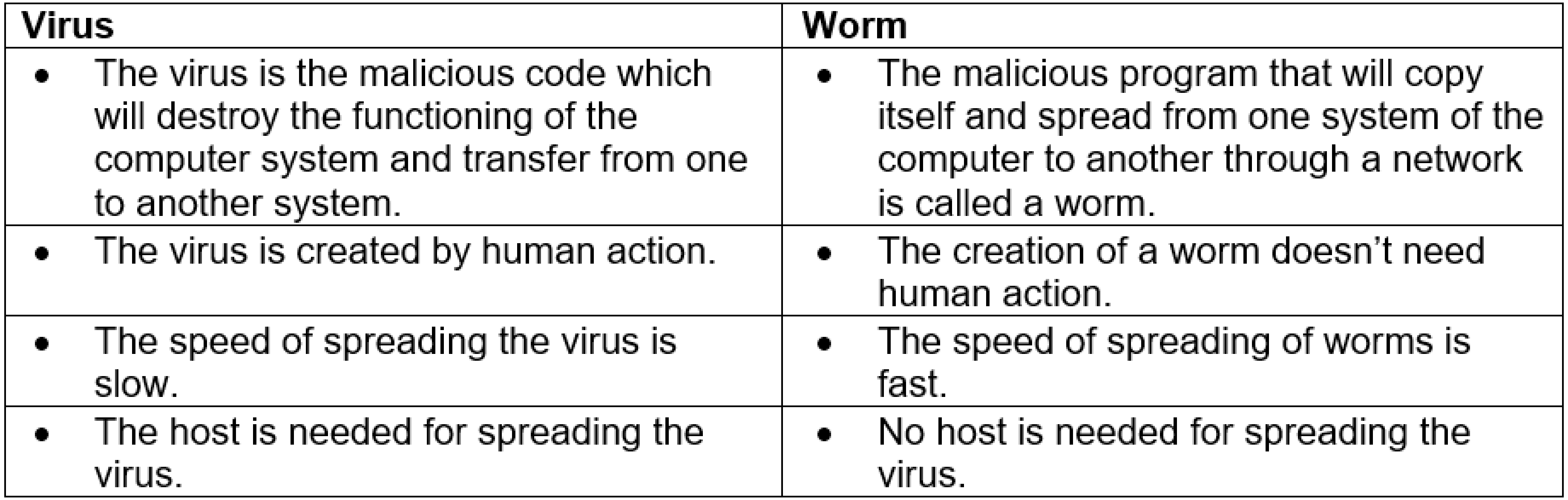
- **It is a type of attack which uses a trial and error method.**

- **This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number.**

- **This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.**

SPAMMING : the sending of multiple unsolicited emails or text messages, usually for marketing purposes

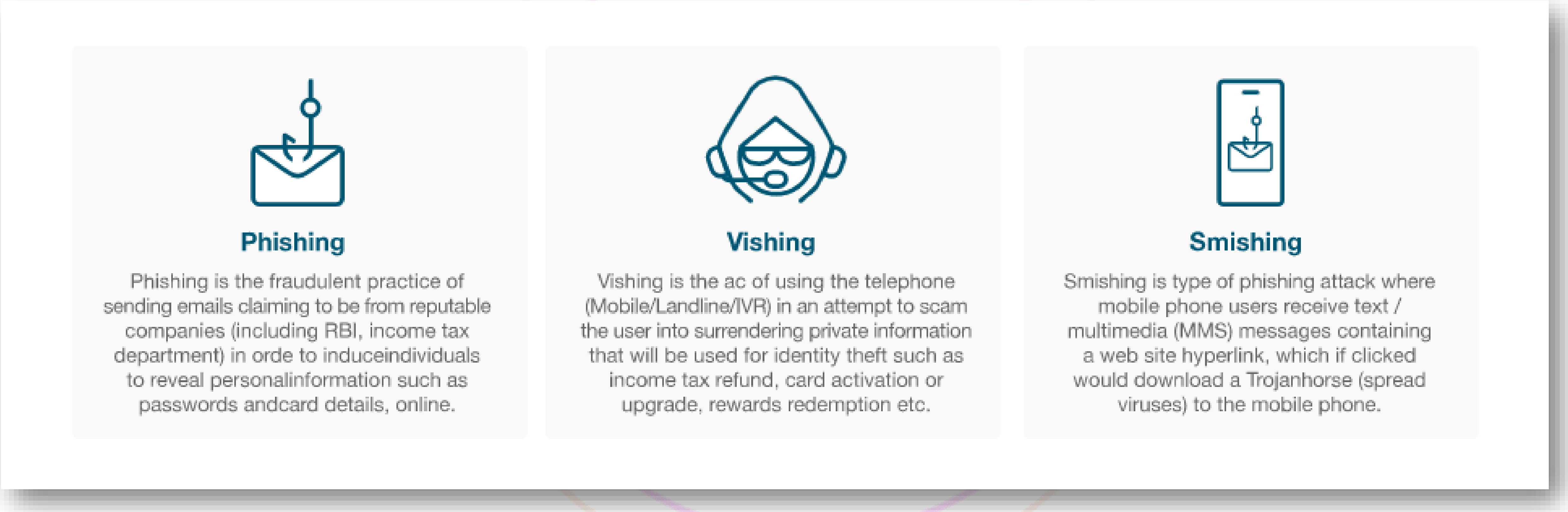
VIRUS : it's a computer program that can self-replicate, infect other programs, and spread to other computers



Virus	Worm
- The virus is the malicious code which will destroy the functioning of the computer system and transfer from one to another system.	- The malicious program that will copy itself and spread from one system of the computer to another through a network is called a worm.
- The virus is created by human action.	- The creation of a worm doesn’t need human action.
- The speed of spreading the virus is slow.	- The speed of spreading of worms is fast.
- The host is needed for spreading the virus.	- No host is needed for spreading the virus.

Phishing

- Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number.
- It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.



Phishing

Phishing is the fraudulent practice of sending emails claiming to be from reputable companies (including RBI, income tax department) in orde to induceindividuals to reveal personalinformation such as passwords andcard details, online.

Vishing

Vishing is the ac of using the telephone (Mobile/Landline/IVR) in an attempt to scam the user into surrendering private information that will be used for identity theft such as income tax refund, card activation or upgrade, rewards redemption etc.

Smishing

Smishing is type of phishing attack where mobile phone users receive text / multimedia (MMS) messages containing a web site hyperlink, which if clicked would download a Trojanhorse (spread viruses) to the mobile phone.

Trojan Horse:

- It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent.
- It appears to be a normal application but when opened/executed some malicious code will run in the background.

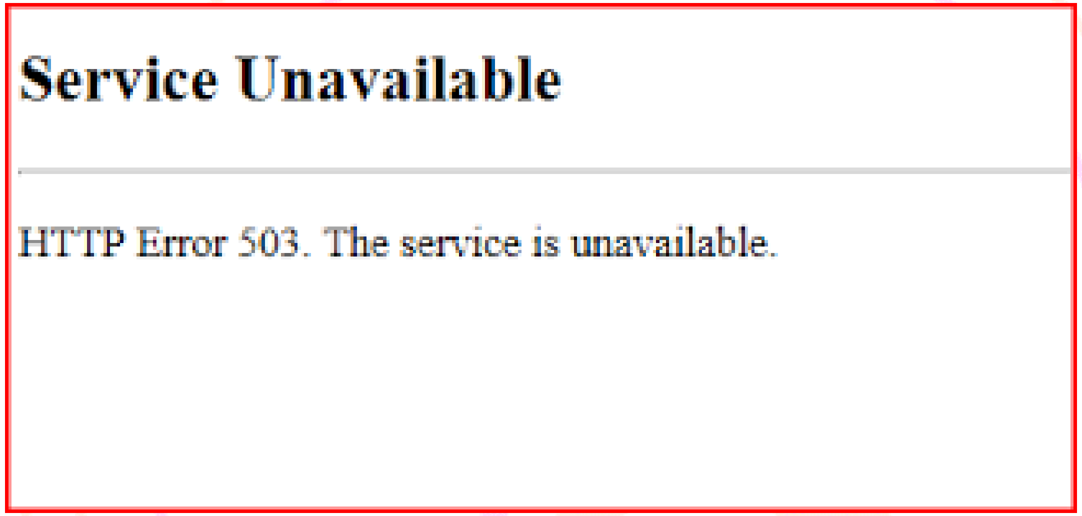
- For example, Trojan horse software observe the e-mail ID and password while entering in web browser for logging.

TEACHERS ADDA BY TARGET ABHI 7877719287

Man-in-the-middle (MitM) attacks:

Also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

Denial of Service attacks:



Service Unavailable

HTTP Error 503. The service is unavailable.

- ➢ A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.
- ➢ DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

Intrusion Detection System (IDS)

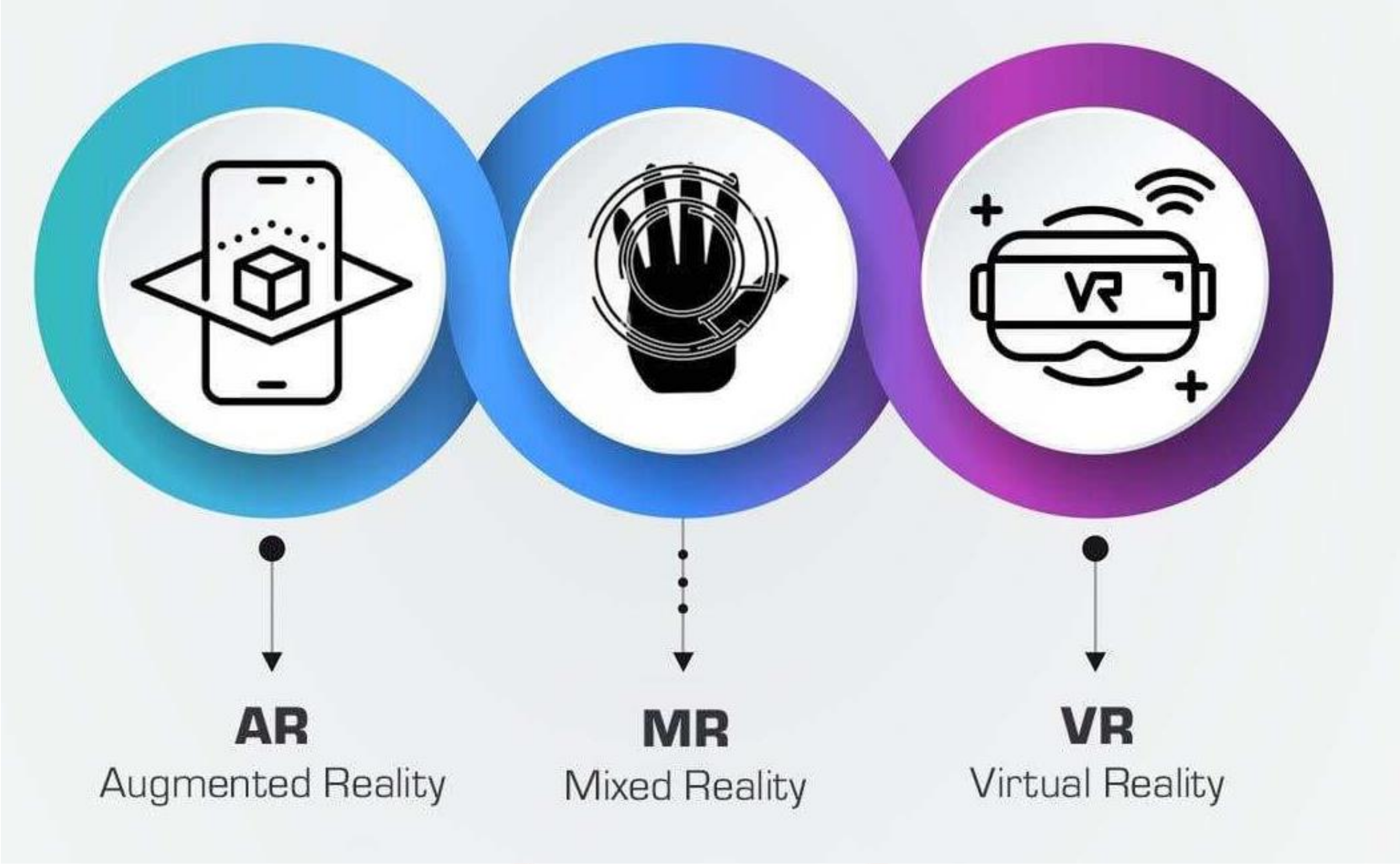
- An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

- It is a software application that scans a network or a system for the harmful activity or policy breaching.

- Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system.

IMMERSIVE TECHNOLOGY

Immersive technology is an integration of virtual content with the physical environment in a way that allows the user to engage naturally with the blended reality.



AR
Augmented Reality

MR
Mixed Reality

VR
Virtual Reality

Virtual reality

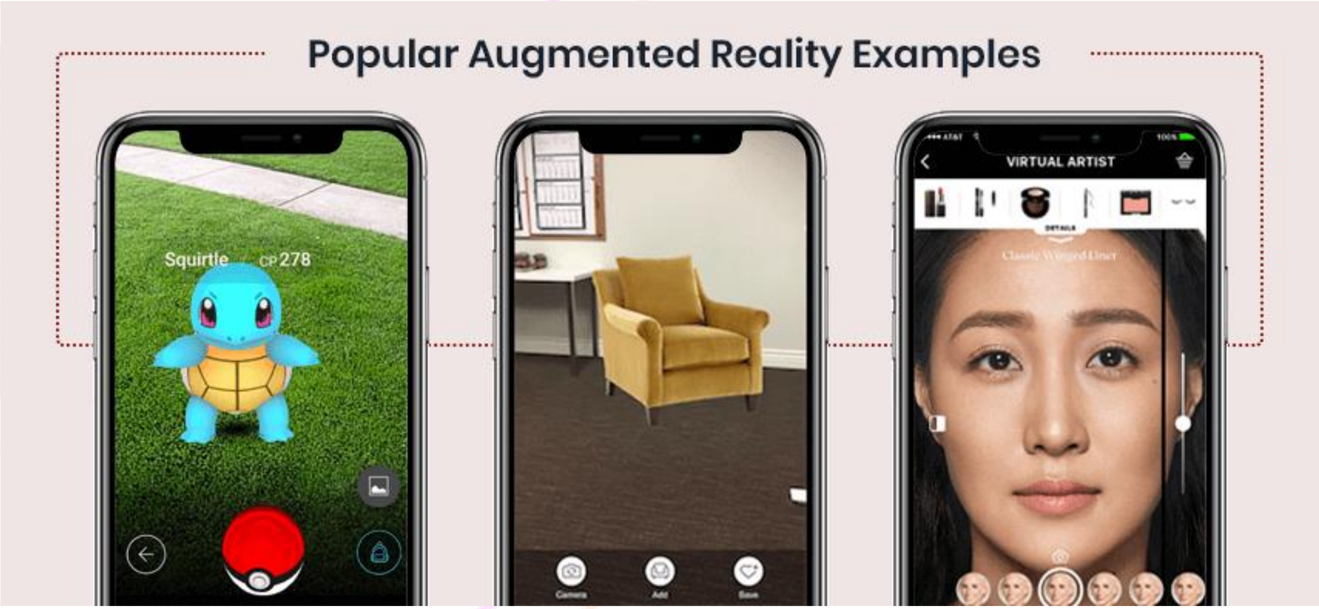
- Virtual reality (VR) refers to a computer-generated simulation in which a person can interact within an artificial three-dimensional environment using electronic devices, such as special goggles with a screen or gloves fitted with sensors.

- In this simulated artificial environment, the user is able to have a realistic-feeling experience.

Augmented Reality

- Augmented reality (AR for short) is defined as "the real-time use of information in the form of text, graphics, audio, or other virtual enhancements integrated with real-world objects.“

- It involves overlaying visual, auditory, or other sensory information onto the world in order to enhance one's experience.

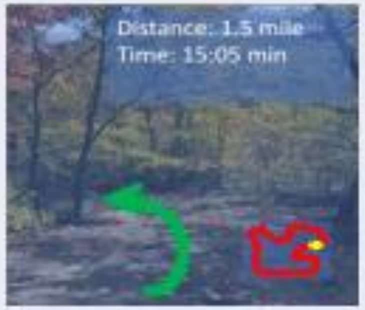
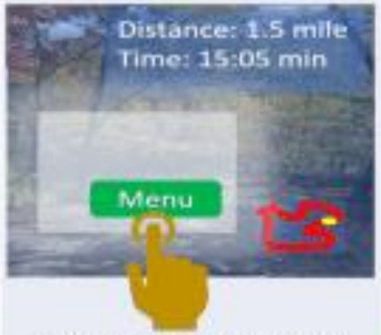

Popular Augmented Reality Examples
Squirtle
CP 278
VIRTUAL ARTIST
Classic Winged Liner

Mixed Reality

- MR brings together real world and digital elements.

- In mixed reality, you interact with and manipulate both physical and virtual items and environments, using next-generation sensing and imaging technologies.

Mixed Reality

		Extended Reality (XR)		
	Reality	Augmented Reality (AR)	Mixed Reality (MR)	Virtual Reality (VR)
Display	Naked eye/optical glasses	Translucent display	Translucent display	Occlusion display
Display example				
Example	 Real view of a trail	 Augmented virtual map and direction	 Interactive virtual contents	 Virtual gaming

Blockchain technology

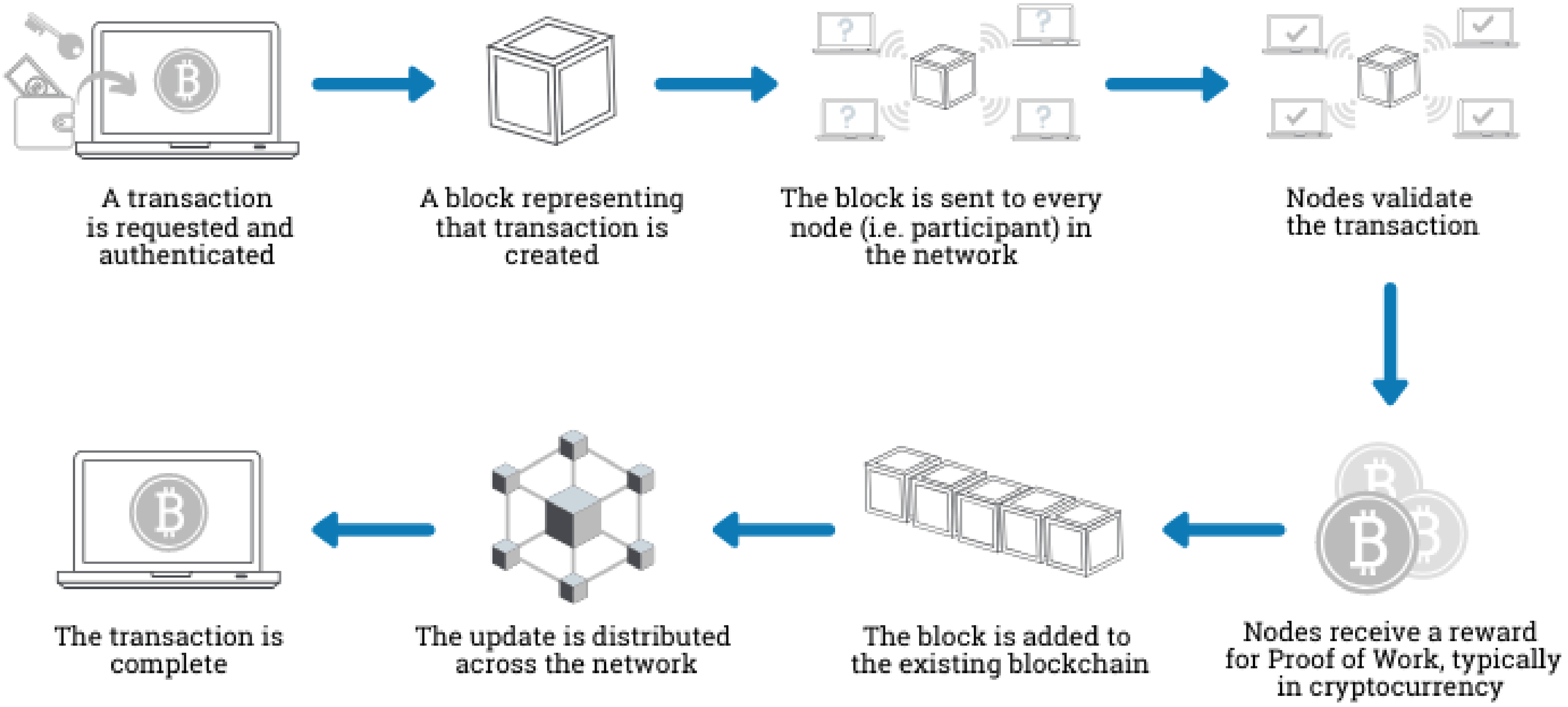
- **Blockchain technology is a decentralized, digital ledger that records transactions across a network of computers.**

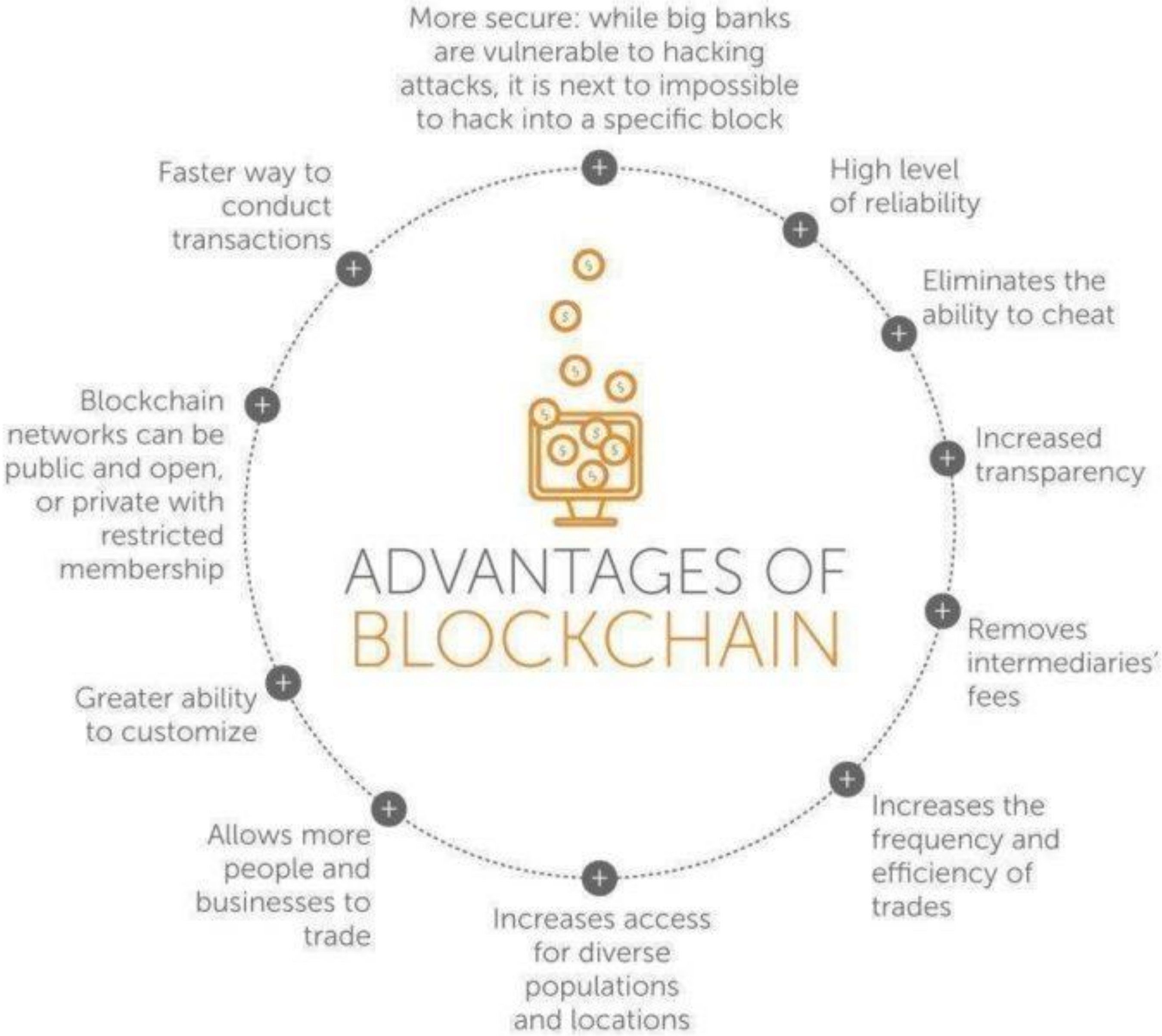
- **Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger.**

Blockchain technology

- The decentralized nature of technology ensures that no single entity can alter or delete previous transactions, providing a high degree of security and transparency.

How does a transaction get into the blockchain?

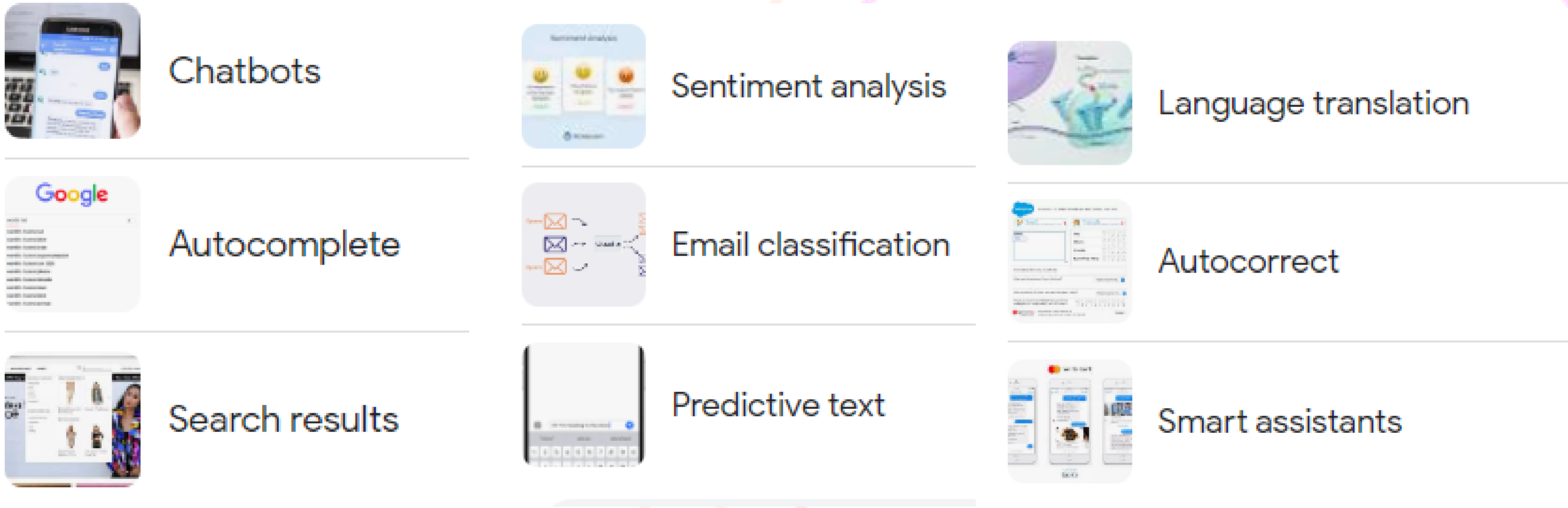

A transaction is requested and authenticated
A block representing that transaction is created
The block is sent to every node (i.e. participant) in the network
Nodes validate the transaction
Nodes receive a reward for Proof of Work, typically in cryptocurrency
The block is added to the existing blockchain
The update is distributed across the network
The transaction is complete



ADVANTAGES OF BLOCKCHAIN

- More secure: while big banks are vulnerable to hacking attacks, it is next to impossible to hack into a specific block
- High level of reliability
- Eliminates the ability to cheat
- Increased transparency
- Removes intermediaries' fees
- Increases the frequency and efficiency of trades
- Increases access for diverse populations and locations
- Allows more people and businesses to trade
- Greater ability to customize
- Blockchain networks can be public and open, or private with restricted membership
- Faster way to conduct transactions

Natural language processing (NLP)



- Chatbots
- Autocomplete
- Search results
- Sentiment analysis
- Email classification
- Predictive text
- Language translation
- Autocorrect
- Smart assistants

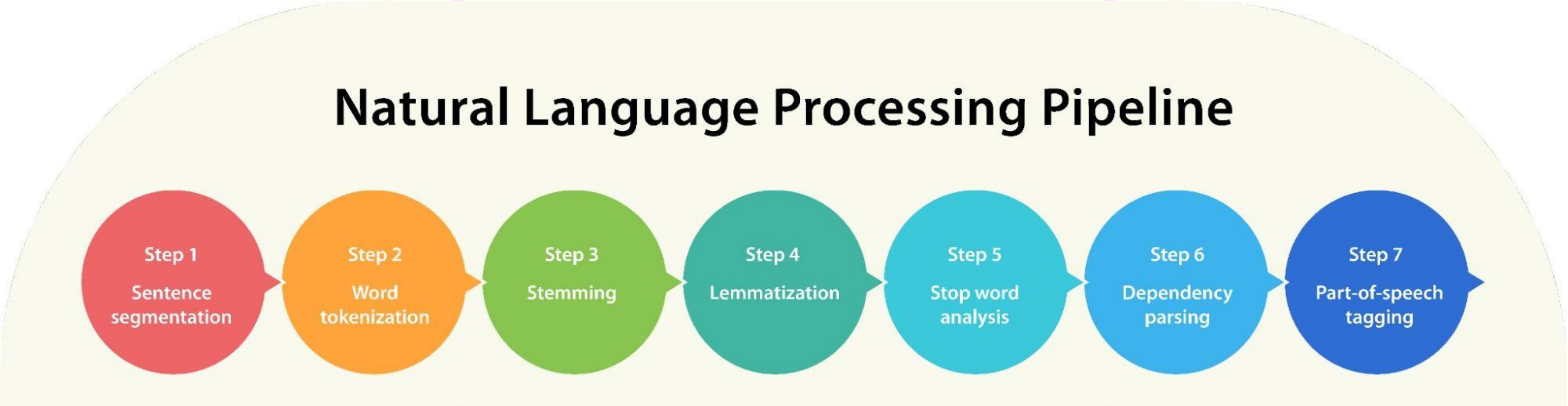
NATURAL LANGUAGE PROCESSING (NLP)

- Natural language processing (NLP) is a subfield of Artificial Intelligence (AI) that deals with the interaction between computers and humans in natural language.

- This technology works on the speech provided by the user breaks it down for proper understanding and processes it accordingly.

- It involves the use of computational techniques to process and analyze natural language data, such as text and speech, with the goal of understanding the meaning behind the language.

NATURAL LANGUAGE PROCESSING (NLP)



Natural Language Processing Pipeline

Step 1 Sentence segmentation

Step 2 Word tokenization

Step 3 Stemming

Step 4 Lemmatization

Step 5 Stop word analysis

Step 6 Dependency parsing

Step 7 Part-of-speech tagging

CLOUD COMPUTING

- Cloud computing means storing and accessing the data and programs on remote servers that are hosted on the internet instead of the computer’s hard drive or local server.

- Cloud computing is also referred to as Internet-based computing.

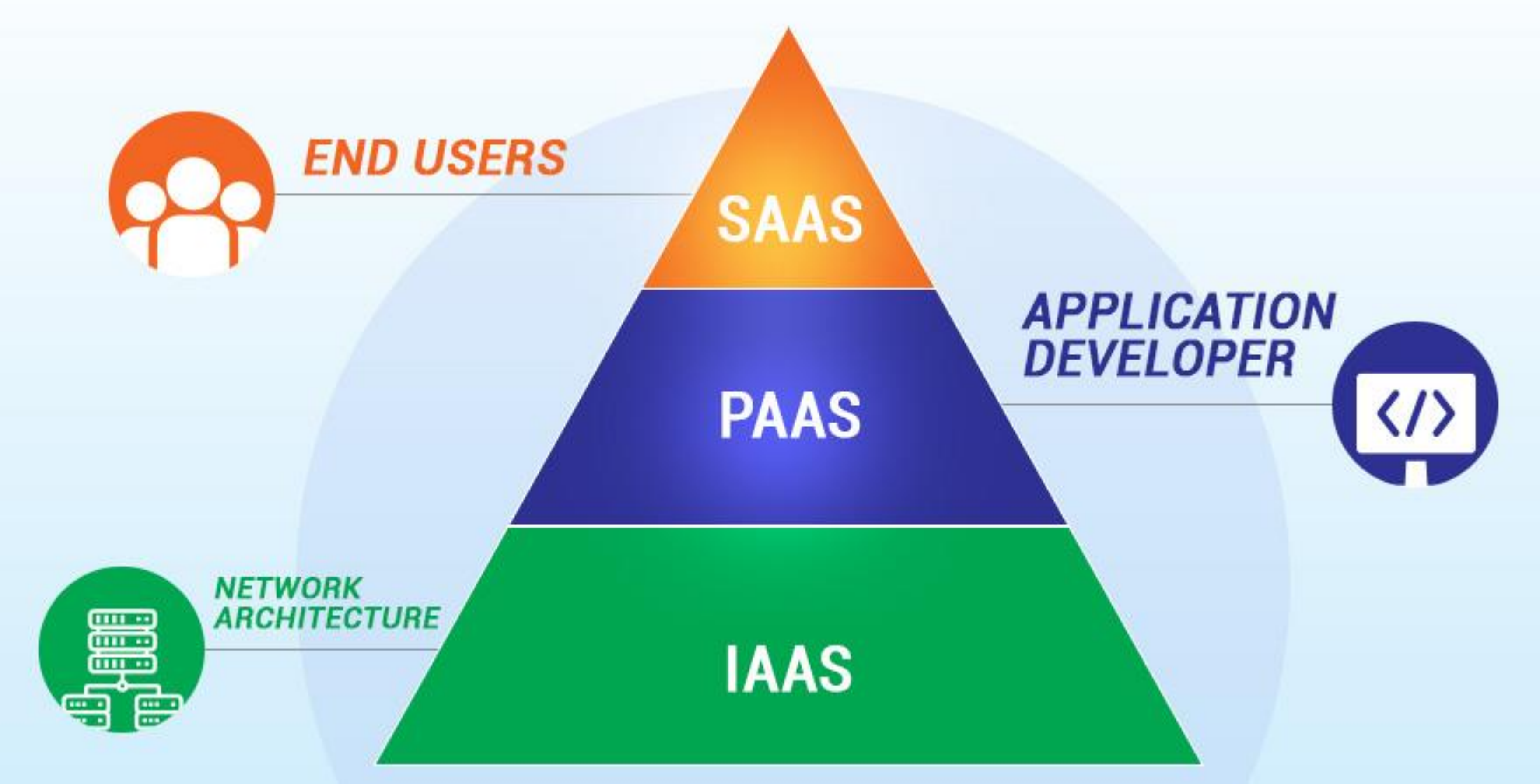
- Cloud computing is the on-demand delivery of IT resources through the internet with pay-to-use charges.

Three Major Cloud Service Models

- Cloud computing services can be broken down into three models

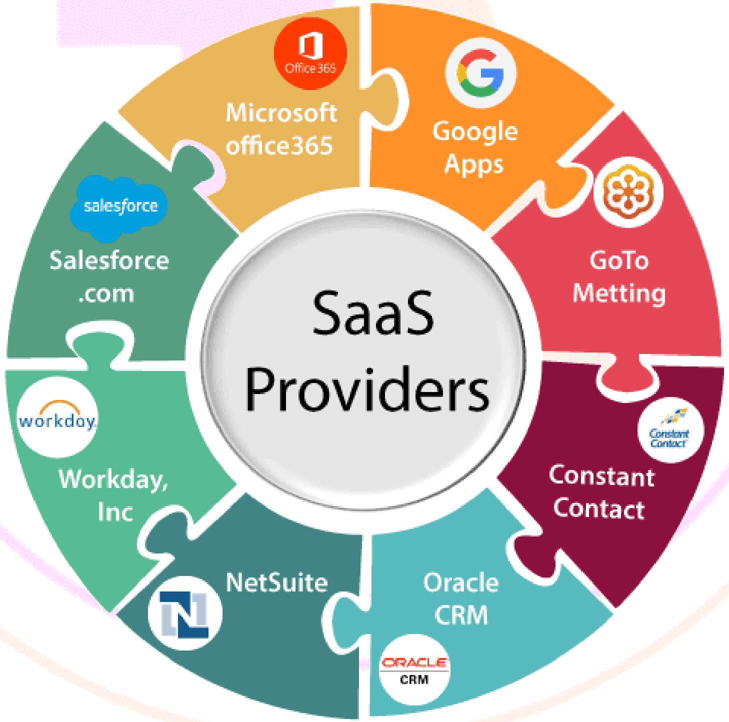
1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

CLOUD COMPUTING

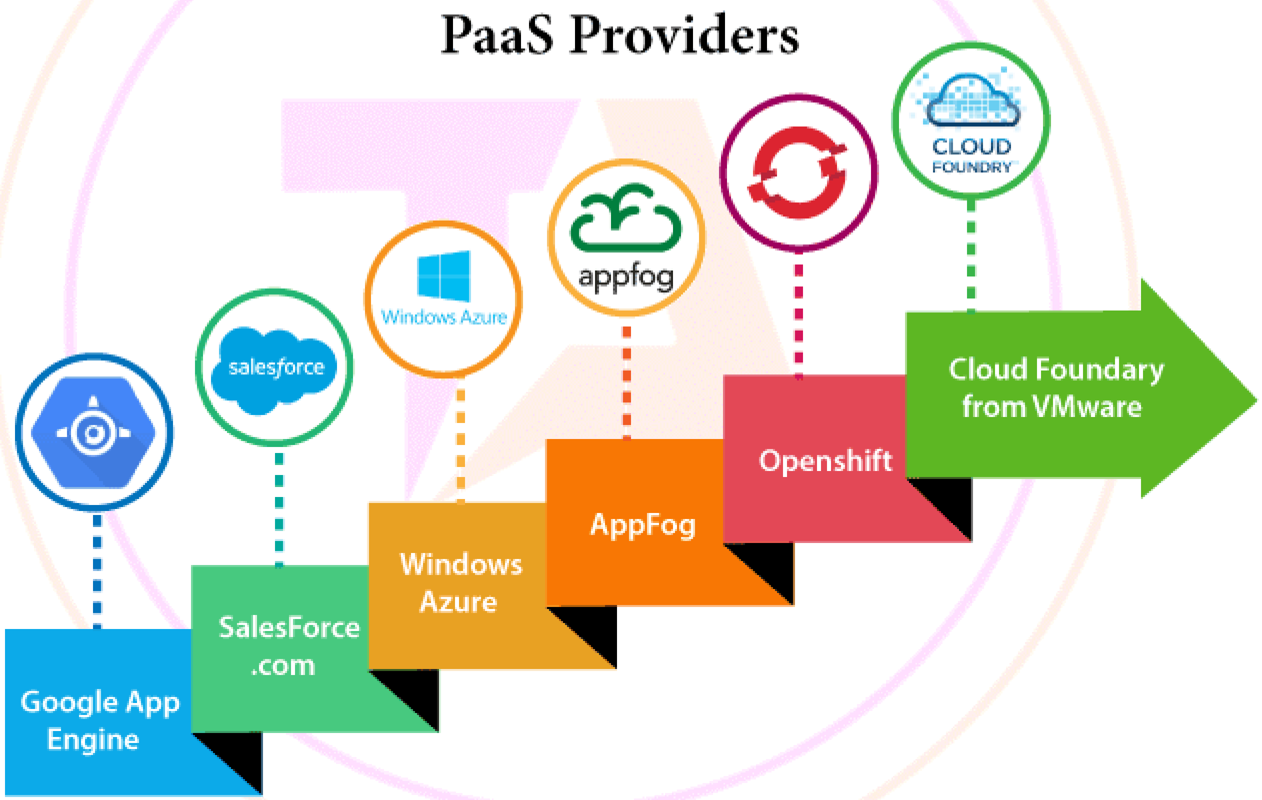


CLOUD COMPUTING

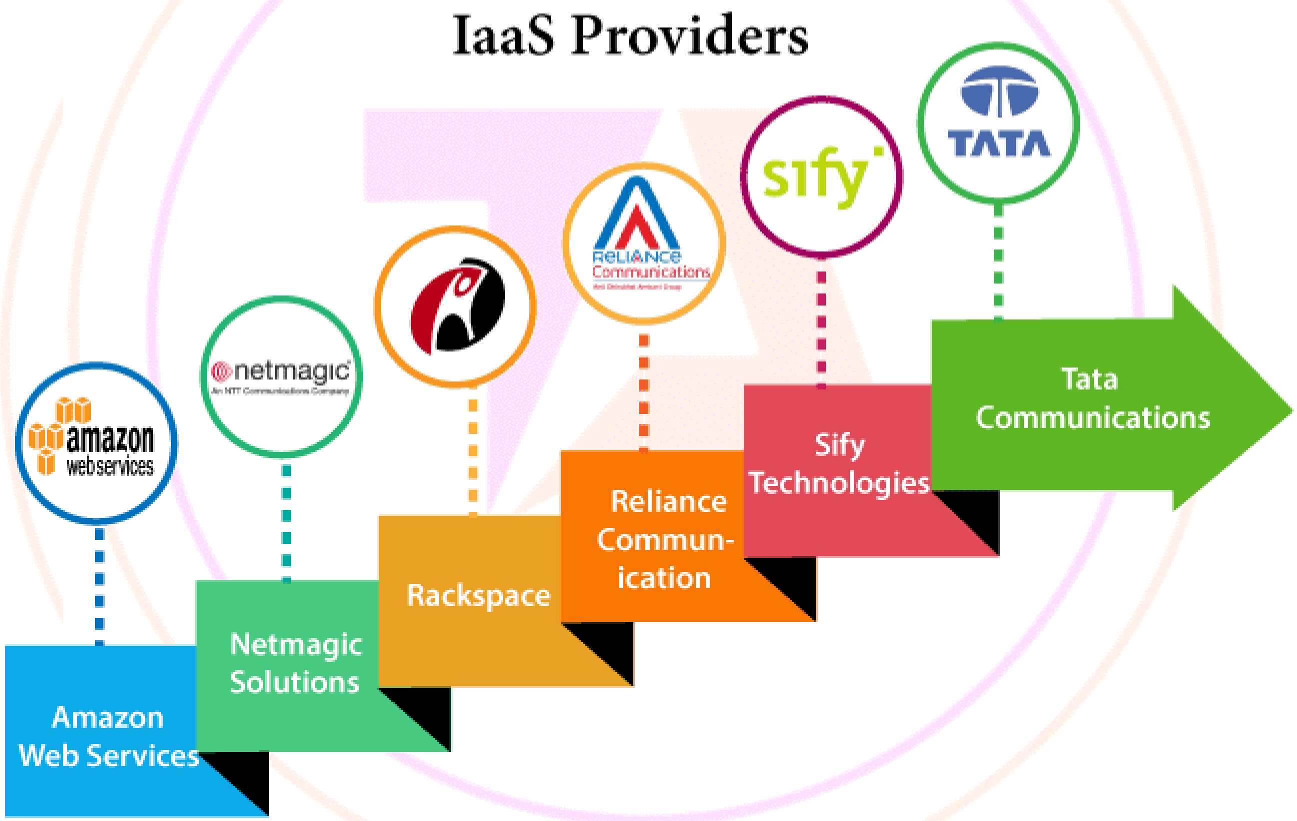
- Software services are offered under a platform.



CLOUD COMPUTING



CLOUD COMPUTING



IaaS Providers

Amazon Web Services

Netmagic Solutions

Rackspace

Reliance Commun-ication

Sify Technologies

Tata Communications

Q. What is the main purpose of virtual reality technology?

a) To create realistic simulations of real-world environments
b) To enhance the gaming experience
c) To improve communication and collaboration in remote teams
d) To enhance the visual effects of movies and television shows

Q. In immersive technology, what does MR stand for?

a) Mixed Reality
b) Measured Reality
c) More Reality
d) Mirrored Reality

Q. What is a blockchain?

1. A blockchain is a centralized digital ledger consisting of records called blocks.
2. A blockchain is a decentralized, distributed, digital ledger consisting of records called blocks.
3. A blockchain is a digital database consisting of records called class.
4. It is a private ledger that no one can inspect.

Q. What is Machine learning?

a) The autonomous acquisition of knowledge through the use of computer programs

b) The autonomous acquisition of knowledge through the use of manual programs

c) The selective acquisition of knowledge through the use of computer programs

d) The selective acquisition of knowledge through the use of manual programs

Q. What is Cloud Computing?

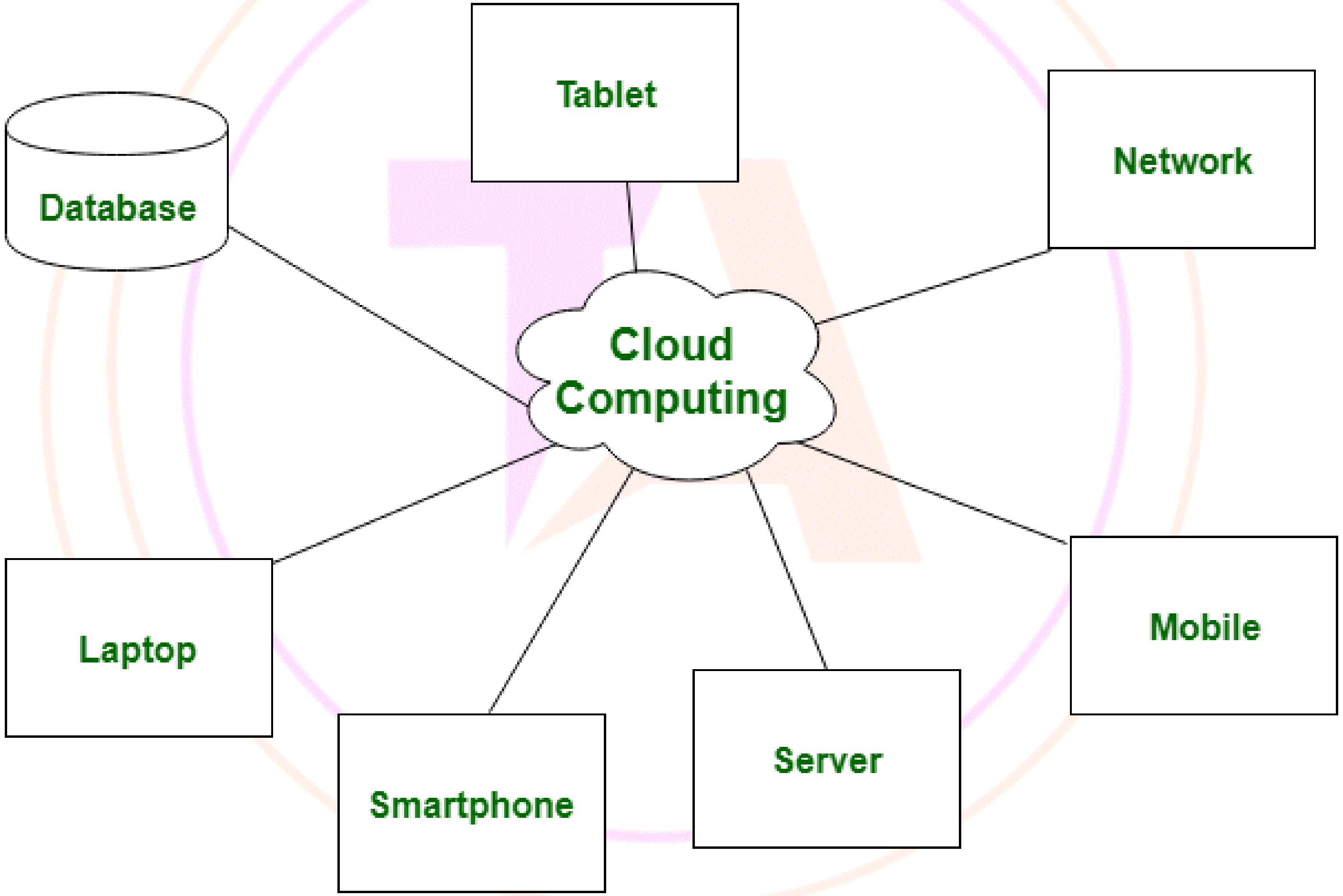
a) Cloud Computing means providing services like storage, servers, database, networking, etc

b) Cloud Computing means storing data in a database

c) Cloud Computing is a tool used to create an application

d) None of the mentioned

CLOUD COMPUTING



TEACHERS ADDA BY TARGET ABHI 7877719287

Grid Computing

- Grid Computing can be defined as a network of computers working together to perform a task that would rather be difficult for a single machine.

- consists of a large number of computers which are connected parallel and forms a computer cluster. This combination of connected computers uses to solve a complex problem.

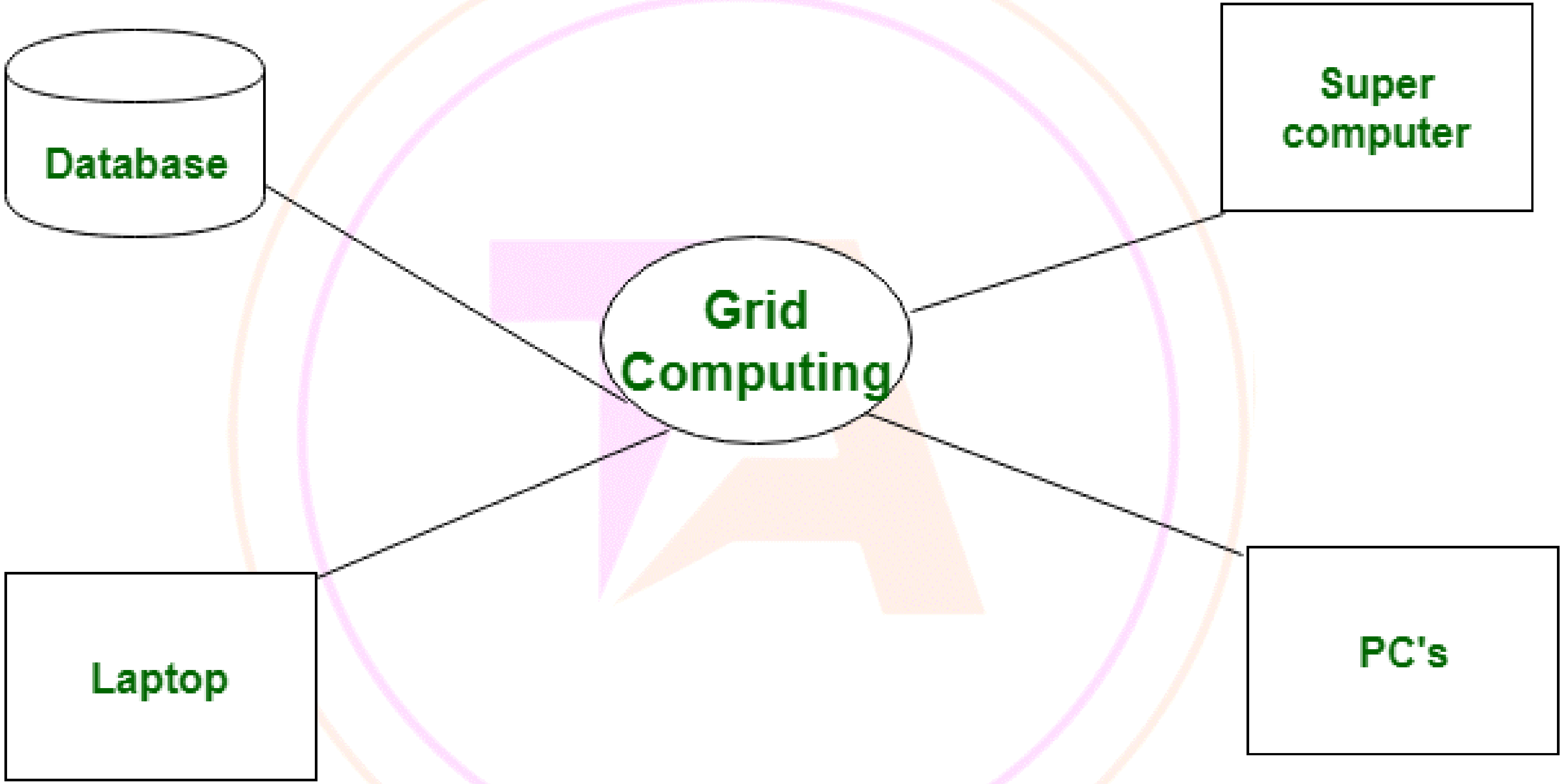
Grid Computing

- The task that they work on may include analyzing huge datasets or simulating situations that require high computing power.

- Computers on the network contribute resources like processing power and storage capacity to the network.

Grid Computing

- A Grid computing network mainly consists of these three types of machines
- **Control Node:** A computer, usually a server or a group of servers which administrates the whole network and keeps the account of the resources in the network pool.
- **Provider:** The computer contributes its resources to the network resource pool.
- **User:** The computer that uses the resources on the network.


Database
Super computer
Grid Computing
Laptop
PC's

What is Big Data Analytics?

- Big data analytics describes the process of uncovering trends, patterns, and correlations in large amounts of raw data to help make data-informed decisions.

- These processes use familiar statistical analysis techniques—like clustering and regression—and apply them to more extensive datasets with the help of newer tools.

What is Big Data Analytics?

- On a broad scale, data analytics technologies and techniques give organizations a way to analyze data sets and gather new information.

- Business intelligence (BI) queries answer basic questions about business operations and performance.

Big data analytics tools and technology

- Big data analytics cannot be narrowed down to a single tool or technology. Instead, several types of tools work together to help you collect, process, cleanse, and analyze big data. Some of the major players in big data ecosystems are listed below.

- Hadoop is an open-source framework that efficiently stores and processes big datasets on clusters of commodity hardware.

- NoSQL databases are non-relational data management systems that do not require a fixed scheme, making them a great option for big, raw, unstructured data.

Big data analytics tools and technology

- MapReduce is an essential component to the Hadoop framework serving two functions. The first is mapping, which filters data to various nodes within the cluster.

- YARN stands for “Yet Another Resource Negotiator.” It is another component of second-generation Hadoop.

Big data analytics tools and technology

- **Spark is an open source cluster computing framework that uses implicit data parallelism and fault tolerance to provide an interface for programming entire clusters.**

- **Tableau is an end-to-end data analytics platform that allows you to prep, analyze, collaborate, and share your big data insights. Tableau excels in self-service visual analysis, allowing people to ask new questions of governed big data and easily share those insights across the organization.**