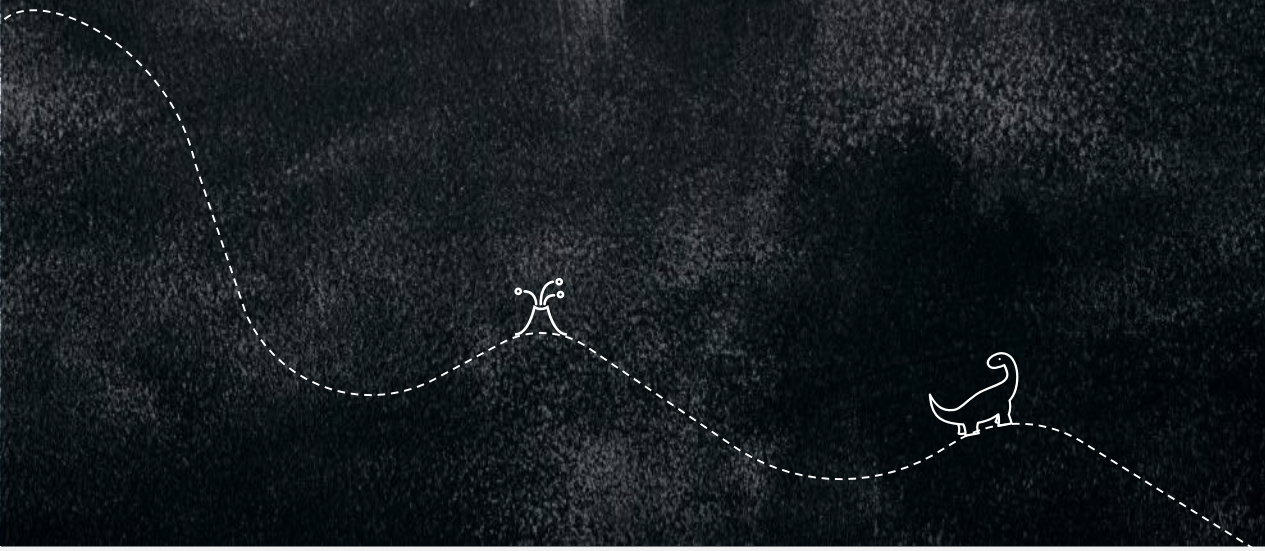
Technologies of Industry 4.0

Big Data



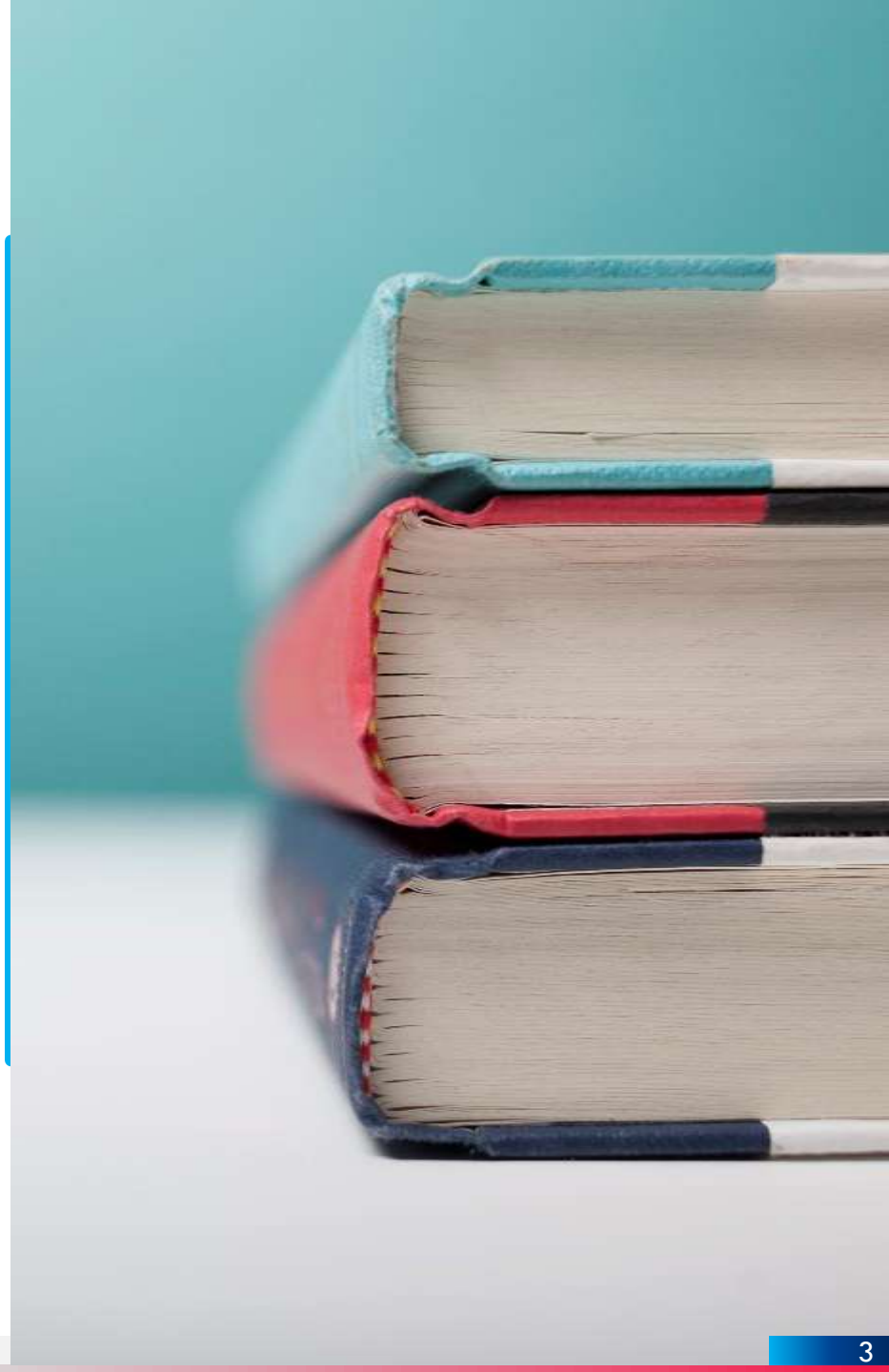
What is Big Data?

It refers to Large, Complex and Diverse sets of Data.

Features of Big Data:

This Big Data is characterized by 5 V's. They are

- Volume
- Velocity
- Variety
- Veracity
- Value



1. **Volume:** Large amount of data (Petabytes, Exabytes)

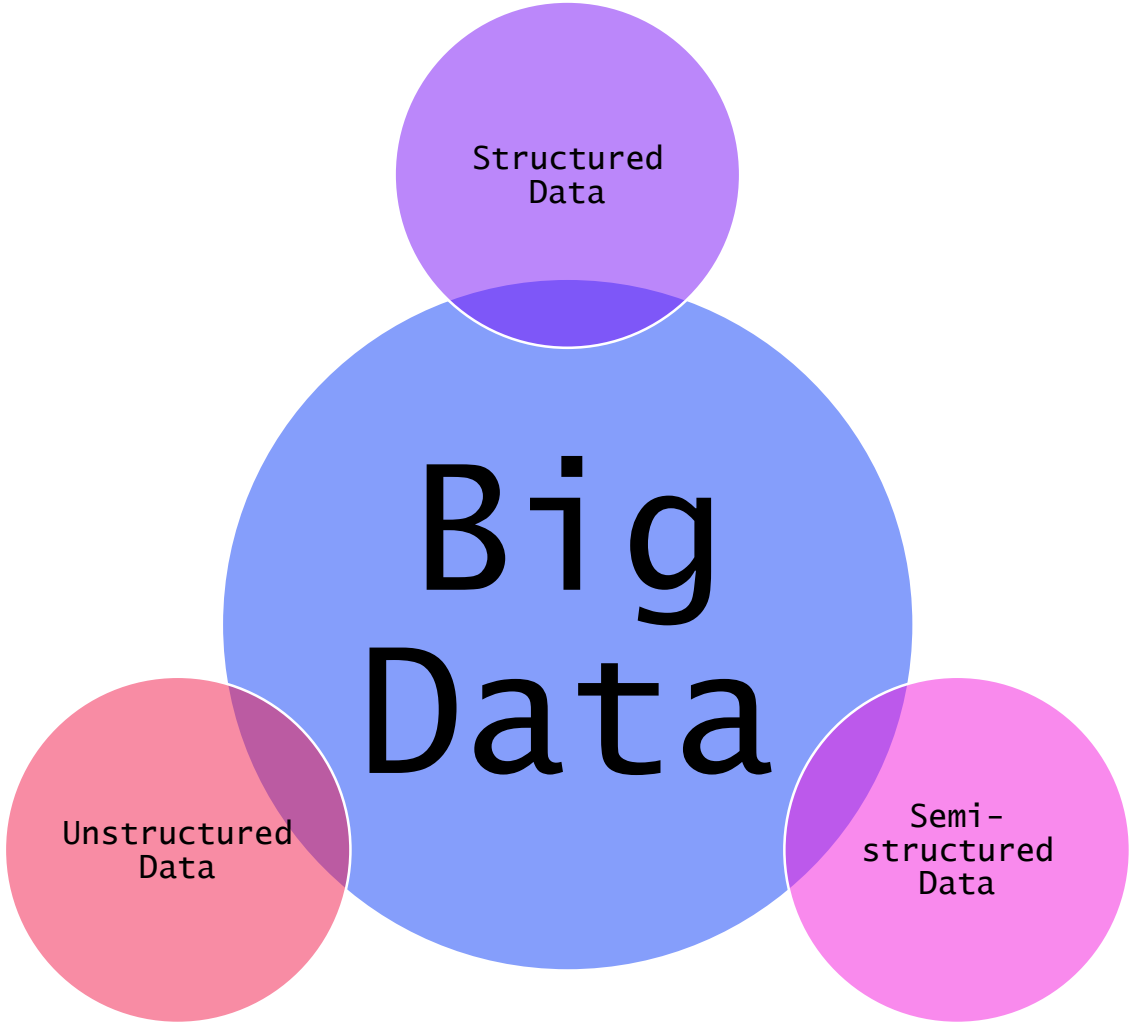
2. **Velocity:** Speed of Transferring Data. (Real-time, Streaming)

3. **Variety:** Diverse data formats & sources (Types of data)

4. **Veracity:** Data accuracy and quality.

5. **Value:** Data's potential to create insights & drive decision-making

Types of Big Data



1. Structured Data:

- Organized and formatted data
- Easily searchable
- Examples: Databases, spreadsheets, CSV files.
- Characteristics: Well defined schema, easy to analyze.

2. Semi-Structured Data:

- Partially organized and formatted data
- Has some level of structure, but lacks a rigid schema.
- Examples: XML, JSON, CSV files with varying formats.
- Characteristics: flexible schema, requires some manual processing for analysis.

3. Unstructured Data:

- Unorganized and unformatted data
- Difficult to search and analyze.
- Examples: Text documents, images, videos, & audio files
- Characteristics: Lack of schema, requires natural language processing (NLP) nor machine learning(ML) for analyze.

Advantages and Disadvantages of Big Data

Advantages

- Improved Decision Making
- Enhanced Customer Insights
- Increased Operational Efficiency
- Better Risk Management.
- New Business Opportunities

Disadvantages

- Data Management Challenges
- Data Quality Issues
- Data Security Risks
- High Costs
- Complexity
- Privacy concerns

Artificial Intelligence

Artificial intelligence refers to the simulation of human intelligence in machines that are programmed to think, learn, and make decisions

Categories of AI

1. **Narrow AI (Weak AI):** Designed to perform a specific task (e.g., voice assistants like Siri, recommendation systems).
2. **General AI (Strong AI):** Machines with the ability to understand, learn, and perform any intellectual task like a human (still theoretical).
3. **Superintelligent AI:** A level of intelligence surpassing human capabilities (a speculative concept).

Applications of AI

- **Healthcare:** Diagnosis, drug discovery, personalized treatment plans.
- **Finance:** Fraud detection, algorithmic trading, risk assessment.
- **Transportation:** Autonomous vehicles, traffic management systems.
- **Entertainment:** Personalized recommendations, content creation.
- **Industry:** Predictive maintenance, automation, supply chain optimization.

Advantages of AI

- Efficiency and automation of repetitive tasks.
- Enhanced decision-making capabilities.
- Scalability and ability to handle large datasets.
- Continuous operation without fatigue.

Challenges

- Ethical issues (bias, privacy, and accountability).
- Potential job displacement due to automation.
- Security risks and misuse of AI technology.

Cybersecurity

Cybersecurity

Cyber security refers to the practice of protecting digital information, networks, and computer systems from unauthorized access/cyber threats.

Types of Cyber Threats

- Malwares
- Phishing
- Ransomware
- SQL Injection
- Cross-site Scripting

1. Malware

Software designed to harm or exploit a computer system.

Types of Malwares

a. **Virus:** A virus is a type of malware that replicates itself by attaching to other programs or files.

b. **Worm:** A worm is a type of malware that can spread from system to system without the need for human interaction.

c. **Trojan:** A Trojan is a type of malware that disguises itself as legitimate software.

d. **Spyware:** Spyware is a type of malware that secretly monitors and collects user data.

e. **Adware:** Adware is a type of malware that displays unwanted advertisements.

2. Phishing

Fraudulent emails, texts, or messages that trick users into revealing sensitive information.

- **Email Phishing:** Email phishing involves sending fake emails that appear to be from a legitimate source.
- **Spear Phishing:** Spear phishing involves targeting specific individuals or groups with tailored phishing attacks.
- **Whaling:** Whaling involves targeting high-level executives or officials with sophisticated phishing attacks.
- **Smishing:** Smishing involves sending phishing messages via SMS or text message.
- **Vishing:** Vishing involves using voice calls to trick users into revealing sensitive information.

3. Ransomware:

Malware that demands payment in exchange for restoring access to encrypted data.

4. SQL Injection:

Attack that injects malicious code into databases to access sensitive information.

5. Cross-Site Scripting (XSS):

Attack that injects malicious code into websites to steal user data.

Cyber Security Measures:

1. **Firewalls:** Network security systems that control incoming and outgoing network traffic.

   Ex: Windows defender firewall, Mac OS X firewall.

2. **Encryption:** Converting data into a code to protect it from unauthorized access.

3. **Strong Passwords:** Using unique, complex passwords for all accounts.

4. **Two-Factor Authentication (2FA):** Requiring a second form of verification, such as a code sent to a phone, in addition to a password.

5. **Regular Software Updates:** Keeping operating systems, applications, and plugins up-to-date with the latest security patches.

Mixed Reality

Mixed Reality (MR):

Mixed Reality (MR) refers to the blending of the physical and digital worlds to create environments where physical and virtual elements coexist and interact in real-time.

Key Characteristics

1. Blending of Real and Virtual Worlds
2. Real-Time Interaction
3. Spatial Awareness

Applications of Mixed Reality

1. **Education and Training**
2. **Healthcare**
3. **Entertainment**
4. **Workplace Collaboration**
5. **Retail and E-commerce**
6. **Architecture and Engineering**
7. **Military and Defence**

Benefits

- Enhanced interactivity
- Improved learning and training
- Collaboration
- Cost savings

Challenges

- Hardware limitations
- Data privacy
- Learning curve
- Development complexity