Parul® University

Subject: Fundamental of Computer Science

Unit-7 CYBER SECURITY AND EMERGING TRENDS

Parul®
University

Topic Cover

- Cyber Security Basics
  - Firewall
  - Encryption
  - Cyber Threats
  - -`Phishing
  - Malware

- Artificial Intelligent and Machine Larning
  - Introduction
  - Real World Application
  - Big Data and Data Science

- Overview of Future Trends in Computing
  - Quantum Computing
  - Edge Computing
  - Blockchain Technology

Parul® University

Cyber Security

- Cybersecurity is the practice of protecting digital information, computer systems, networks, and data from theft, damage, or unauthorized access through technologies, processes, and practices

- It ensures the confidentiality, integrity, and availability of data by defending against threats like malware, phishing, and ransomware using tools such as firewalls and encryption.

- Cybersecurity involves physical and operational security, end-user education, and disaster recovery planning to safeguard digital assets and maintain business continuity.

Parul®
University

DIGITAL LEARNING CONTENT

Cyber Security

Parul®
University

Cyber Security

- **Confidentiality**: Ensures that data is not accessed by unauthorized individuals. This is achieved through measures like access controls, encryption, and multi-factor authentication.

- **Integrity**: Guarantees that data is accurate, complete, and has not been tampered with. This is maintained through error-checking, version control, and digital signatures.

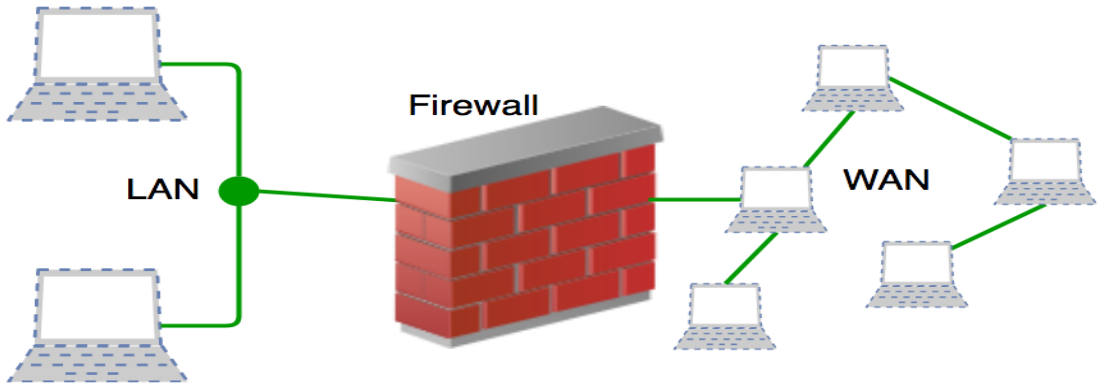
- **Availability**: Ensures that authorized users can access the information and systems when they need them. This is supported by system redundancy, disaster recovery plans, and regular maintenance.

Parul® University

DIGITAL LEARNING CONTENT

Firewalls

- A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on a set of predetermined security rules.
- It acts as a barrier between a trusted network, like a private network or a single computer, and an untrusted network, such as the internet, to protect against unauthorized access and cyber threats. Firewalls can be hardware, software, or a combination of both.



Parul® University

Firewalls

How it works—

- **Monitors traffic**: A firewall inspects data packets as they enter and exit a network.
- **Applies rules**: It compares each packet against a set of security rules to determine if it should be allowed or blocked.
- **Blocks threats**: By following these rules, it can prevent malicious traffic, unauthorized access, and other cyberattacks from reaching the network.
- **Manages traffic:** It can also be used for other purposes, such as content filtering to block access to certain websites.

Parul® University

DIGITAL LEARNING CONTENT

Firewalls

Types of firewalls—

- **Hardware firewalls:** These are dedicated physical devices that sit between a network and the internet, often used in corporate environments to protect an entire network.
- **Software firewalls:** These are applications installed on individual computers and can be found on operating systems like Windows and macOS.
- **Combination:** Many businesses use both types for a layered approach to security.

Parul® University

DIGITAL LEARNING CONTENT

Encryption

- Encryption is the process of converting readable data (plaintext) into an unreadable format (ciphertext) to protect it from unauthorized access.
- This is achieved using a cryptographic key, which is a set of mathematical values that allows for the data to be both encoded and decoded.
- Decryption is the reverse process, which converts the ciphertext back into its original, readable form.

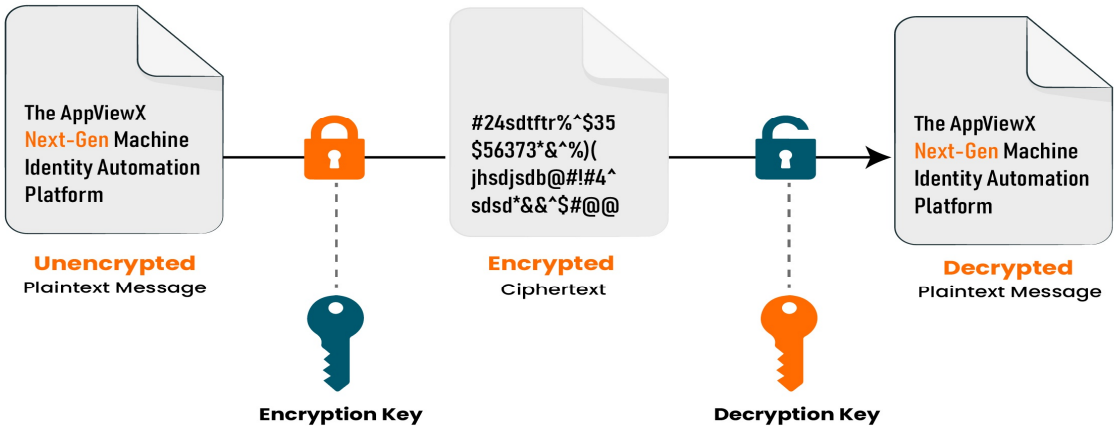
Parul® University

DIGITAL LEARNING CONTENT

Encryption

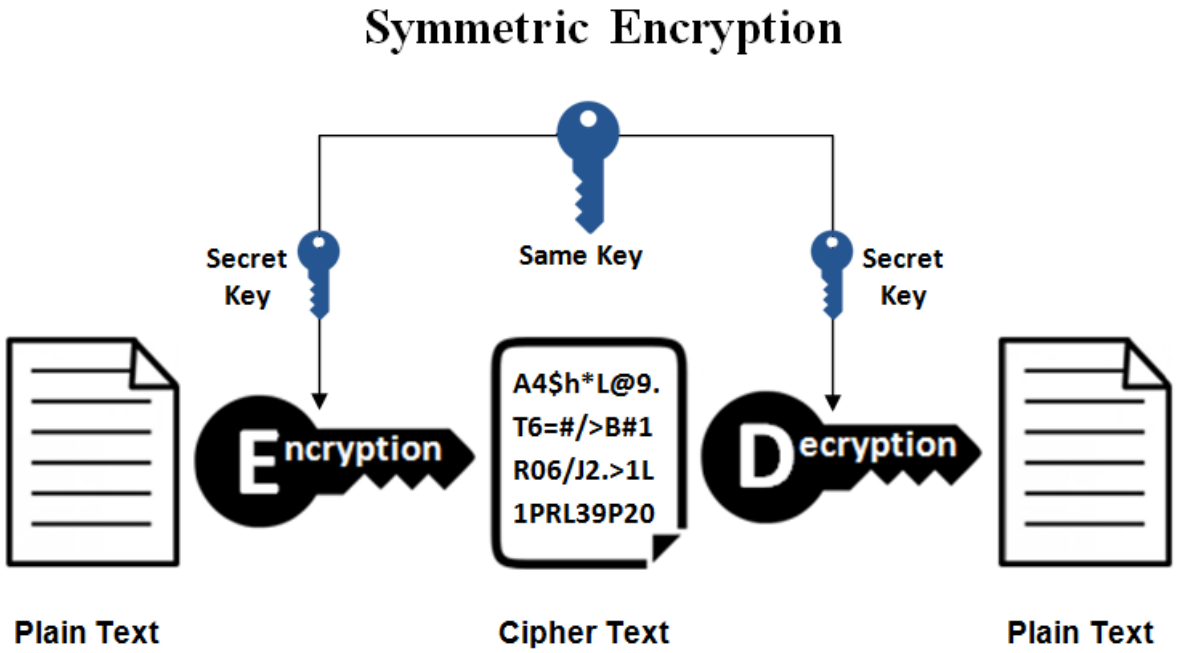
Encoding: An algorithm, along with a key, scrambles readable data into a jumbled, unreadable format. For example, a simple Caesar cipher might shift each letter of a message forward by a set number of places in the alphabet.

Decoding: The recipient, who possesses the correct key, uses the same or a corresponding algorithm to reverse the process, turning the ciphertext back into the original plaintext.



Encryption

Symmetric encryption: Uses a single, shared secret key for both encryption and decryption. It is known for being fast, but requires secure key exchange

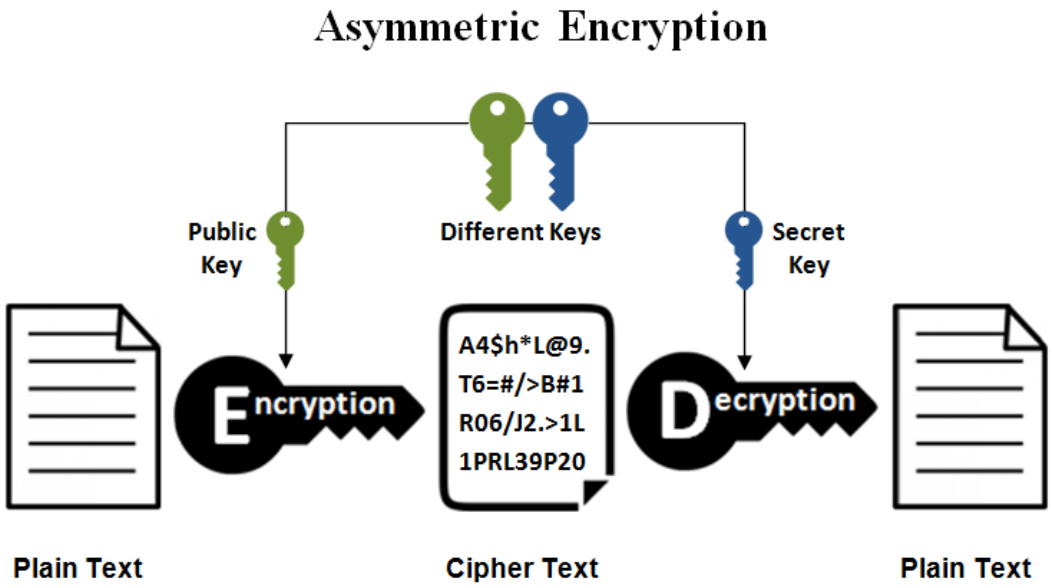


Parul® University

DIGITAL LEARNING CONTENT

Encryption

Asymmetric encryption: Uses a pair of keys: a public key for encryption and a private key for decryption. This is more secure for sharing information, as the public key can be shared widely, while the private key is kept secret.



Why Encryption Important

- **Data security**: It's a fundamental tool for protecting data from theft and misuse, especially for sensitive information like financial and personal details.
- **Secure communication**: Ensures that communications remain confidential, even if intercepted, by using techniques like end-to-end encryption.
- **Data integrity**: Can verify that data has not been altered or tampered with during transit or while stored.
- **Regulatory compliance:** Helps organizations in industries like healthcare and finance meet strict data protection regulations.
- **Consumer trust:** Using encryption can build trust with customers, showing a commitment to protecting their data.

Parul® University

DIGITAL LEARNING CONTENT

Cyber Threats

- Cyber threats are malicious attempts to access, damage, steal data, or disrupt digital systems and operations.
- Common types include malware, ransomware, phishing, denial-of-service (DDoS) attacks, and insider threats. These threats can lead to unauthorized access, data breaches, financial loss, and disruption of business.
- Cyber threats also refer to the possibility of a successful cyber attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or any other form of sensitive data.
- Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.

Parul® University

DIGITAL LEARNING CONTENT

Cyber Threats

Parul® University

DIGITAL LEARNING CONTENT

Cyber Threats

Common types of cyber threats

- **Malware**: Malicious software, such as viruses, worms, and spyware, designed to infiltrate and harm computer systems, steal data, or compromise integrity and availability.
- **Ransomware**: A type of malware that encrypts a victim's files and demands a ransom for their decryption.
- **Phishing**: Social engineering attacks that use deceptive emails, messages, or websites to trick individuals into revealing sensitive information like passwords or credit card numbers.

Parul® University

DIGITAL LEARNING CONTENT

Cyber Threats

Common types of cyber threats

- **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks:** Attacks that overwhelm a system, server, or network with a flood of internet traffic, making it unavailable to users.

- **Insider Threats:** Malicious acts or security risks created by people within an organization who have authorized access to systems and data, such as employees or contractors.

- **Social Engineering:** A broad category of attacks that manipulates people into giving up confidential information or performing actions that compromise security.

Cyber Threats

Common types of cyber threats

- **Man-in-the-Middle (MitM) attacks:** An attacker secretly intercepts and relays communication between two parties who believe they are directly communicating with each other.

- **Code Injection Attacks:** Attacks where malicious code is "injected" into an application or system, which can be used to execute commands or steal data (e.g., SQL injection).

Parul® University

DIGITAL LEARNING CONTENT

Cyber Threats

Consequences of cyber threats:

- Unauthorized access to sensitive data
- Destruction or corruption of computer systems
- Financial losses due to theft, fraud, or system downtime
- Damage to reputation and loss of customer trust
- Disruption of essential economic activities

Phishing Attack

- A phishing attack is a type of cyberattack where malicious actors impersonate trusted entities to trick people into revealing sensitive information like passwords, credit card details, or social security numbers.

- Attackers use deceptive emails, text messages, or fake websites to create a sense of urgency or trust, compelling victims to click malicious links, download harmful files, or share their data. These attacks rely on social engineering to exploit human psychology rather than technical vulnerabilities.

Parul® University

DIGITAL LEARNING CONTENT

Phishing Attack

Parul® University

DIGITAL LEARNING CONTENT

Phishing Attack

How it works

- **Impersonation:** The attacker pretends to be a legitimate source, such as a bank, a well-known company, or even a personal acquaintance.
- **Deceptive communication:** They use emails, text messages (smishing), phone calls (vishing), or social media messages to contact the victim.
- **Psychological manipulation:** The messages often create a sense of urgency, fear, or curiosity to manipulate the victim into acting quickly without thinking.
- **Malicious payload:** The attack typically involves a link that leads to a fake website designed to steal credentials or a malicious file that, when opened, installs malware.

Malware

- Malware, or malicious software, is a type of software designed to disrupt, damage, or gain unauthorized access to computer systems.
- It is used for harmful purposes like stealing data, obtaining financial information, or extorting payments.
- Common types of malware include viruses, worms, Trojan horses, spyware, adware, and ransomware, which spread through various vectors such as phishing emails, malicious websites, and infected files.

Parul® University

DIGITAL LEARNING CONTENT

Artificial Intelligent and Machine Learning

- AI is the overarching term for any technology that enables computers to perform tasks that typically require human intelligence, such as reasoning, problem-solving, and decision-making.

- To perform tasks that would normally require human intelligence, like problem-solving or decision-making.

- ML is a subset of AI that allows systems to learn from data and improve over time without being explicitly programmed.

- To identify patterns in data and use those patterns to make predictions or decisions about new data, improving over time.

Parul®
University

DIGITAL LEARNING CONTENT

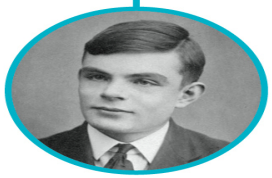
Artificial Intelligent and Machine Learning

1642 — First mechanical calculating machine built by French mathematician and inventor Blaise Pascal.

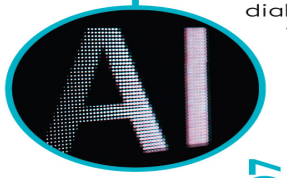
1837 — First design for a programmable machine, by Charles Babbage and Ada Lovelace.

1943 — Foundations of neural networks established by Warren McCulloch and Walter Pitts, drawing parallels between the brain and computing machines.

1950 — Alan Turing introduces a test—the Turing test—as a way of testing a machine's intelligence.



1955 — 'Artificial intelligence' is coined during a conference devoted to the topic.



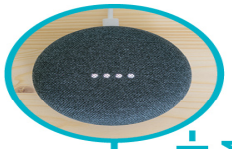
1965 — ELIZA, a natural language program, is created. ELIZA handles dialogue on any topic; similar in concept to today's chatbots.

1980s — Edward Feigenbaum creates expert systems which emulate decisions of human experts.

1997 — Computer program Deep Blue beats world chess champion Garry Kasparov.

2002 — iRobot launches Roomba, an autonomous vacuum cleaner that avoids obstacles.

2009 — Google builds the first self-driving car to handle urban conditions.



2011 — IBM's Watson defeats champions of US game show Jeopardy!

2011-2014 — Personal assistants like Siri, Google Now, Cortana use speech recognition to answer questions and perform simple tasks.

2014 — Ian Goodfellow comes up with Generative Adversarial Networks (GAN).

2016 — AlphaGo beats professional Go player Lee Sedol 4–1.

2018 — Most universities have courses in Artificial Intelligence.

Parul®
University

DIGITAL LEARNING CONTENT

Artificial Intelligent and Machine Learning

The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Parul® University

DIGITAL LEARNING CONTENT

Artificial Intelligent and Machine Learning

Core AI technologies

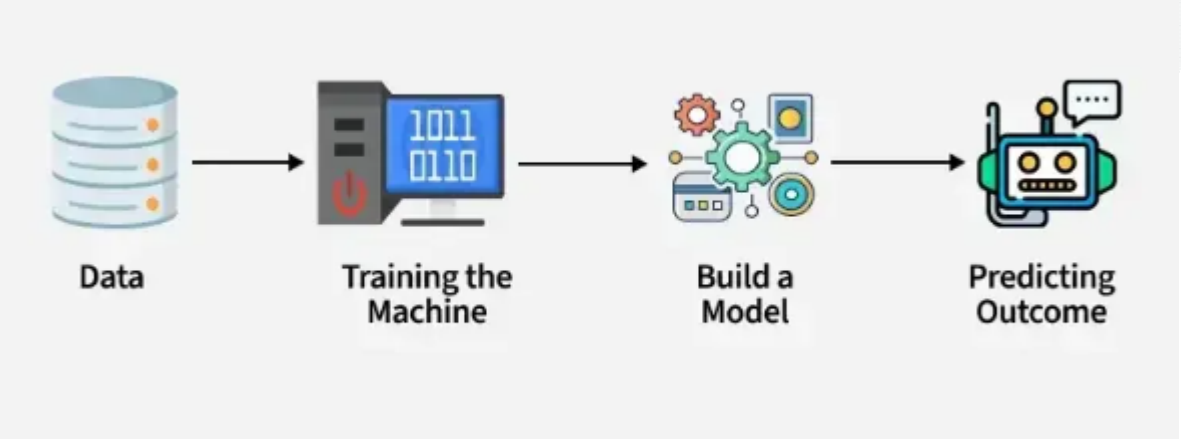
- Machine Learning: A subset of AI where systems learn from data to find patterns and make predictions.
- Deep Learning: A type of machine learning that uses multi-layered neural networks to solve complex problems.
- Natural Language Processing (NLP): Enables computers to understand, interpret, and generate human language.
- Computer Vision: Allows machines to "see" and interpret visual information from images or videos.

Parul®
University

DIGITAL LEARNING CONTENT

Artificial Intelligent and Machine Learning

Machine learning (ML) allows computers to learn and make decisions without being explicitly programmed. It involves feeding data into algorithms to identify patterns and make predictions on new data. It is used in various applications like image recognition, speech processing, language translation, recommender systems, etc. In this article, we will see more about ML and its core concepts.



Parul® University

DIGITAL LEARNING CONTENT

Artificial Intelligent and Machine Learning

Why do we need Machine Learning?

1. Solving Complex Business Problems
2. Handling Large Volumes of Data
3. Automate Repetitive Tasks
4. Personalized User Experience
5. Self Improvement in Performance

Parul® University

Artificial Intelligent and Machine Learning

Real World Application of AI and ML

- Virtual assistants: Tools like Siri, Alexa, and Google Assistant use natural language processing to understand and act on voice commands.
- Email filtering: ML algorithms automatically move unwanted emails to a spam folder.
- Image and speech recognition: This is used for facial recognition in smartphones, transcribing speech, and voice commands.
- Recommendation engines: Platforms like Netflix, YouTube, and Amazon use ML to suggest movies, videos, and products based on user behavior.

Parul® University

DIGITAL LEARNING CONTENT

Artificial Intelligent and Machine Learning

Real World Application of AI and ML

- Fraud detection: Banks and financial institutions use ML to identify and flag suspicious transactions in real-time.
- Personalized marketing: ML helps companies understand consumer behaviour, segment audiences, and target advertisements more effectively.
- Chatbots: AI-powered chatbots provide 24/7 customer support by answering frequently asked questions.
- Algorithmic trading: Machine learning is used in finance to analyse market trends and make automated trading decisions.

Parul® University

Artificial Intelligent and Machine Learning

Real World Application of AI and ML

- Medical diagnosis: ML aids doctors in diagnosing diseases from medical images like X-rays and MRIs.
- Personalized treatment: AI can help personalize treatment plans based on a patient's specific data.
- Personalized learning: Educational platforms use ML to adapt lessons to a student's progress, learning style, and weaknesses.

Parul® University

DIGITAL LEARNING CONTENT

Artificial Intelligent and Machine Learning

Real World Application of AI and ML

- Self-driving cars: AI uses sensors and algorithms to navigate roads and make driving decisions.
- Traffic prediction: Applications like Google Maps use ML to predict traffic congestion and suggest optimal routes.
- Predictive maintenance: In manufacturing, ML can predict when machinery is likely to fail, allowing for maintenance before a breakdown occurs.

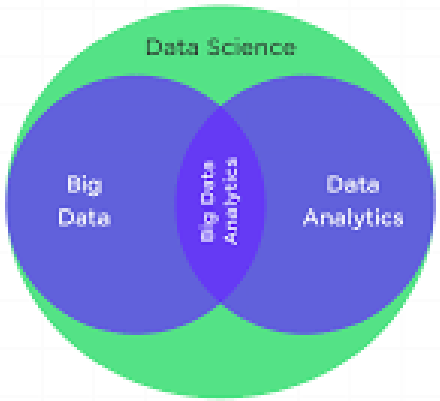
Parul® University

DIGITAL LEARNING CONTENT

Big Data and Data Science

- Data science is the process of extracting insights from data, while Big Data refers to the massive, complex datasets themselves and the technologies needed to process them.

- Data science uses scientific methods, statistics, and machine learning to analyse data, often including Big Data, to make predictions and inform decisions. Big Data provides the raw material, and data science provides the methods to analyse it.



Parul® University

DIGITAL LEARNING CONTENT

Big Data and Data Science

Data science

- Goal: To extract knowledge and insights from data to help with decision-making through scientific methods, algorithms, and systems.
- Focus: A cross-disciplinary field that involves data extraction, preparation, analysis, and visualization.
- Tools: Common tools include programming languages like Python and R, SQL, and machine learning libraries.
- Skills: Requires expertise in statistics, math, machine learning, and domain knowledge.

Parul® University

DIGITAL LEARNING CONTENT

Big Data and Data Science

Big Data

- Goal: To efficiently store, process, and analyse large, complex datasets that are too large for traditional databases.
- Focus: Characterized by the "three Vs": high volume, high velocity, and high variety of information assets.
- Tools: Requires specialized technologies like Hadoop, Spark, NoSQL databases, and cloud computing platforms.
- Skills: Requires knowledge of distributed systems, parallel computing, and data engineering.

Parul® University

DIGITAL LEARNING CONTENT

Big Data and Data Science

The relationship between data science and Big Data

- Complementary, not the same: Data science is the overarching field, and Big Data is a specialized area within it.

- Foundation and application: Big Data provides the large-scale data that data science analyses.

Example: Healthcare organizations use Big Data to collect massive amounts of patient data. Data scientists then use this data to build predictive models that can help forecast disease outbreaks or personalize treatment plans.

Big Data and Data Science

The relationship between data science and Big Data

- Complementary, not the same: Data science is the overarching field, and Big Data is a specialized area within it.

- Foundation and application: Big Data provides the large-scale data that data science analyses.

Example: Healthcare organizations use Big Data to collect massive amounts of patient data. Data scientists then use this data to build predictive models that can help forecast disease outbreaks or personalize treatment plans.

Parul® University

DIGITAL LEARNING CONTENT

Future Trends in Computing

- Future trends in computing include Quantum Computing, which tackles complex problems in areas like drug discovery and cryptography; Blockchain, which creates secure, decentralized ledgers for finance, supply chains, and data management; and Edge Computing, which processes data closer to its source to reduce latency and enable real-time applications.

- These technologies will revolutionize industries by offering unprecedented computational power, enhancing security and transparency, and enabling faster, more responsive systems.

Parul® University

DIGITAL LEARNING CONTENT

Future Trends in Computing

Quantum Computing:

A new paradigm of computing that uses quantum-mechanical phenomena like superposition and entanglement to perform calculations far beyond the reach of classical computers.

Future trends in QC

- Solving complex problems: Breakthroughs in drug discovery, materials science, and complex simulations by modelling molecules and systems with high accuracy.

Parul® University

DIGITAL LEARNING CONTENT

Future Trends in Computing

- Cryptography: Revolutionizing encryption techniques for enhanced security, while also posing a threat to current encryption methods, leading to the development of quantum-resistant cryptography.
- Optimization: Solving complex optimization problems in logistics, finance, and traffic flow.
- Accessibility: The development of "quantum cloud computing" will make this technology accessible to a wider range of businesses and researchers.

Parul® University

DIGITAL LEARNING CONTENT

Future Trends in Computing

Blockchain

A decentralized, immutable, and transparent digital ledger that records transactions across many computers, making the data secure and resistant to tampering.

Future trends:

- Decentralized Finance (DeFi): Driving innovation in financial services like lending, borrowing, and trading without traditional intermediaries.

Future Trends in Computing

- Supply chain management: Increasing transparency and traceability for products as they move from origin to consumer.
- Digital identity and verification: Providing secure, verifiable digital identities and streamlining processes like digital rights management.
- Smart contracts: Automating agreements and transactions as soon as predefined conditions are met.

Parul® University

DIGITAL LEARNING CONTENT

Future Trends in Computing

Edge Computing:

A distributed computing paradigm that brings computation and data storage closer to the sources of data, rather than relying solely on a centralized cloud.

Future trends:

- Real-time processing: Enabling real-time data processing and analysis for applications like autonomous vehicles, industrial automation, and smart city infrastructure.

Parul® University

DIGITAL LEARNING CONTENT

Future Trends in Computing

- Reduced latency: Decreasing delays in communication between devices and the cloud, which is crucial for applications requiring immediate responses.
- IoT growth: Supporting the massive increase in data generated by the Internet of Things (IoT) by processing and filtering it locally.
- Enhanced security: By processing sensitive data locally, edge computing can reduce the amount of data that needs to be transmitted to the cloud, potentially improving security and privacy.

DIGITAL LEARNING CONTENT

Parul® University

www.paruluniversity.ac.in