

DIGITAL FULENCY

Faculty: Prof. Akshatha S

DATA BASE MANAGEMENT SYSTEM (DBMS)

MEANING OF DATA:

Data are individual facts, statistics or items of information, often numeric, that are collected through observation. The word “data” is the plural form of the word “datum” which means “fact”. Therefore, data is a collection of facts.

Database: Collection of data is database, which contains information relevant to the enterprise.

Database Management: A DBMS is a collection of programs that allows data to be stored, reformed and extracted from a database. Database Management allows a person to organize, store and retrieve data from a computer. Database Management can also describe the data storage, operations, and security practices of a database administrator (DBA) throughout the life cycle of the data.

TYPES OF DATABASE:

1. **Relational database:** It is the most efficient way to access structured information. The data is organized into a set of tables that has columns and rows.
2. **Object-oriented database:** Here, the data is represented in the form of objects, as in object-oriented programming.
3. **Distributed database:** It has two or more files located in different places. The database may be in the same physical location on multiple computers or scattered over different networks.
4. **NoSQL database:** NoSQL is a nonrelational database that contains unstructured and semistructured data. It rose in popularity as web applications came to be commonly used and became more complex.
5. **Graph database:** It stores data in the form of entities and the relationships between them.
6. **Cloud database:** This database runs on a Cloud Computing platform, and access is provided ‘as a service.’
7. **Centralization database:** CDB is located, stored, and maintained in a single centralized location, for example, a mainframe computer, desktop, or server CPU.
8. **Operational database:** Also known as OLTP or online transactional processing database, it is designed to create or update big amounts of data and store transactions performed by multiple users in real-time.
9. **Data warehouses:** It is a central repository for data. It holds current and historical data in a single location for analytical reporting throughout the enterprise.

ADVANTAGES OF DATABASES:

- Minimum data redundancy
- Improved data security
- Increased consistency
- Lower updating errors
- Reduced costs of data entry, data storage, and data retrieval
- Improved data access using host and query languages
- Higher data integrity from application programs

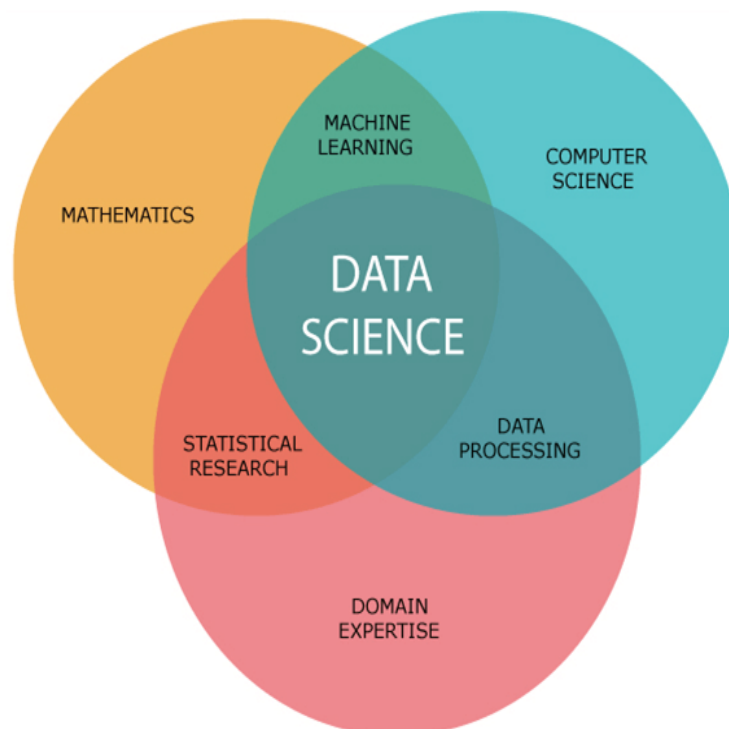
APPLICATIONS OF DATABASE:

Field	Application
Railways	Reservation information, tickets, train schedules, etc.
Library	Book information, issue date, etc.
Banking	Client information, account, activities, loans, etc.
Education	Student information, courses, grades, etc.
Credit card exchange	Card information, charges, etc.
Social Media	User data, demographics, preferences, etc.
Broadcast	User information, bills, etc.
Accounts	Account information, transactions, etc.
ECommerce	Inventory information, purchases, invoices, etc.
HR Management	Employee information, salary, paychecks, etc.
Manufacturing	Supplier information, bills, inventory, etc.
Airline	Flight information, schedules, etc.

DATA SCIENCE:

It is area of study which involves extracting insights from vast amounts of data by the use of various scientific methods, algorithms and processes. It helps you to discover hidden patterns from the raw data. The term data science has emerged because of the evolution of mathematical statistics, data analysis and big data. It is an interdisciplinary field that allows you to extract knowledge from structured or unstructured data.

DATA SCIENCE COMPONENTS:



1. Statistics: Statistics is one of the most important components of data science. Statistics is a way to collect and analyze the numerical data in a large amount and finding meaningful insights from it.

2. Domain Expertise: In data science, domain expertise binds data science together. Domain expertise means specialized knowledge or skills of a particular area.

3. Data engineering: Data engineering is a part of data science, which involves acquiring, storing, retrieving, and transforming the data. Data engineering also includes metadata (data about data) to the data.

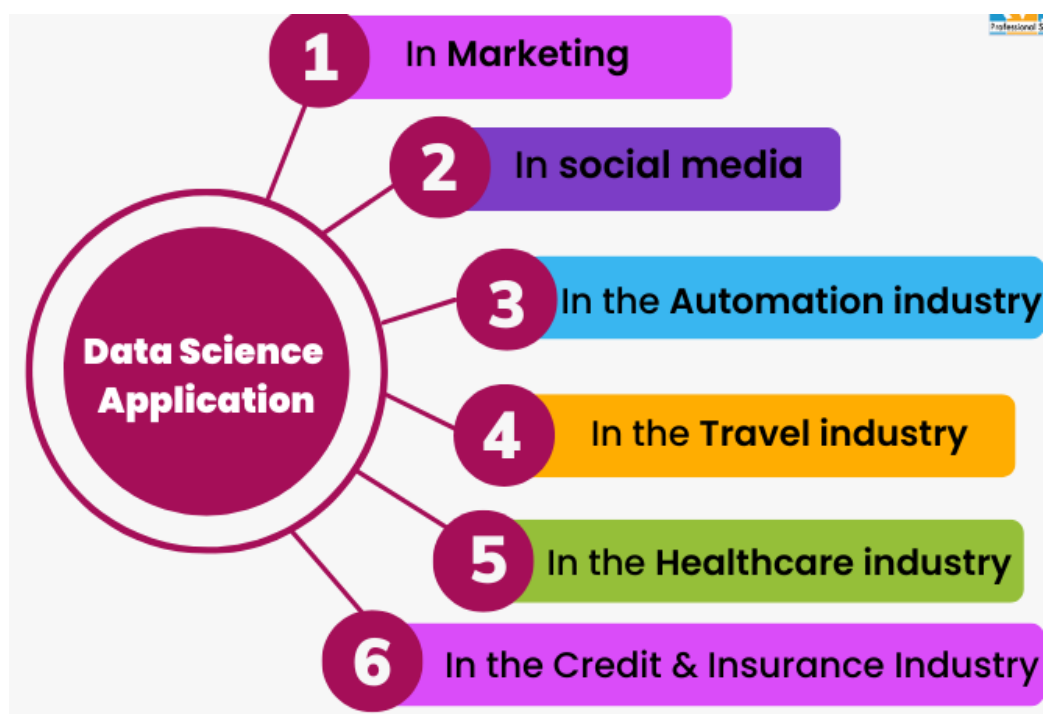
4. Visualization: Data visualization is meant by representing data in a visual context so that people can easily understand the significance of data. Data visualization makes it easy to access the huge amount of data in visuals.

5. Advanced computing: Heavy lifting of data science is advanced computing. Advanced computing involves designing, writing, debugging, and maintaining the source code of computer programs.

6. Mathematics: Mathematics is the critical part of data science. Mathematics involves the study of quantity, structure, space, and changes.

7. Machine learning: Machine learning is backbone of data science. Machine learning is all about to provide training to a machine so that it can act as a human brain.

APPLICATIONS OF DATA SCIENCE:



- In Marketing, Data Science is used for getting valuable customer insights, real-time interactions, customer segmentation, targeting, cross-selling, and predicting the lifetime value of a customer.
- In Sales, Data Science is used for future sales prediction, discount offers, etc.
- In social media, Data Science is used for measuring marketing performance KPIs, monitoring the effectiveness of campaigns, creating personalized ads, sentiment analysis, and much more.
- In the Automation industry, Data Science is used for self-driven cars.
- In the Travel industry, Data Science is applied to predicting flight delays and dynamic pricing.
- In the Healthcare industry, Data Science is applied for medication effectiveness and the prediction of diseases.

- In the Credit & Insurance Industry, Data Science detects fraud and risks and is also used for claims prediction.

BIG DATA ANALYTICS

Introduction: Big data- Analytics

Big data: The definition of big data is data that contains greater variety, arriving in increasing volumes and with more velocity. This is also known as the three Vs. Put simply, big data is larger, more complex data sets, especially from new data sources. These data sets are so voluminous that traditional data processing software just can't manage them.

Big data- Analytics:

Big data analytics is the process of collecting, examining, and analysing large amounts of data to discover market trends, insights, and patterns that can help companies make better business decisions. This information is available quickly and efficiently so that companies can be agile in crafting plans to maintain their competitive advantage.

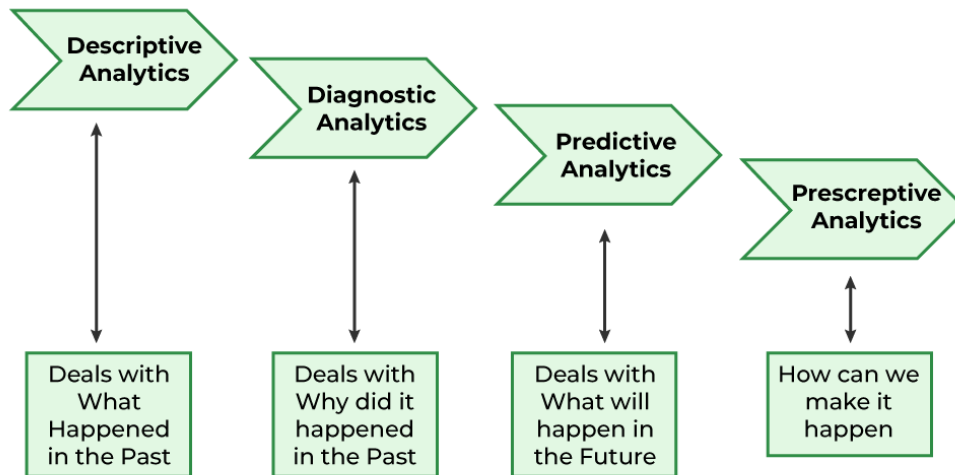
For example, big data analytics is integral to the modern health care industry. As you can imagine, systems that must manage thousands of patient records, insurance plans, prescriptions, and vaccine information.

It can help organizations to better understand the information contained within the data. It also helps to identify the data that is most important to the business and future business decisions. Analysts working with Big Data typically want the knowledge that comes from analysing the data.

TYPES OF BIG DATA ANALYTICS

There are four major types of data analytics:

1. Predictive (forecasting)
2. Descriptive (business intelligence and data mining)
3. Prescriptive (optimization and simulation)
4. Diagnostic analytics



1. **Predictive Analytics:** Predictive analytics turn the data into valuable, actionable information. predictive analytics uses data to determine the probable outcome of an event or a likelihood of a situation occurring.
2. **Descriptive Analytics:** Descriptive analytics looks at data and analyze past event for insight as to how to approach future events. It looks at past performance and understands the performance by mining historical data to understand the cause of success or failure in the past.
3. **Prescriptive Analytics:** Prescriptive Analytics automatically synthesize big data, mathematical science, business rule, and machine learning to make a prediction and then suggests a decision option to take advantage of the prediction.
4. **Diagnostic Analytics:** In this analysis, we generally use historical data over other data to answer any question or for the solution of any problem. We try to find any dependency and pattern in the historical data of the particular problem.

BENEFITS OF BIG DATA ANALYTICS

- **Cost reduction:** Big data can reduce costs in storing all business data in one place. Tracking analytics also helps companies find ways to work more efficiently to cut costs wherever possible.
- **Product development:** Developing and marketing new products, services, or brands is much easier when based on data collected from customers' needs and wants. Big data analytics also helps businesses understand product viability and to keep up with trends.
- **Strategic business decisions:** The ability to constantly analyse data helps businesses make better and faster decisions, such as cost and supply chain optimisation.
- **Customer experience:** Data-driven algorithms help marketing efforts (targeted ads, for example) and increase customer satisfaction by delivering an enhanced customer experience.

- **Risk management:** Businesses can identify risks by analysing data patterns and developing solutions for managing those risks.

APPLICATIONS OF BIG DATA ANALYTICS

- **Entertainment:** Providing a personalised recommendation of movies and music according to a customer's preferences has been transformative for the entertainment industry (think Spotify and Netflix).
- **Education:** Big data helps schools and educational technology companies develop new curriculums while improving existing plans based on needs and demands.
- **Health care:** Monitoring patients' medical histories helps doctors detect and prevent diseases.
- **Government:** Big data can be used to collect data from CCTV and traffic cameras, satellites, body cameras and sensors, emails, calls, and more, to help manage the public sector.
- **Marketing:** Customer information and preferences can be used to create targeted advertising campaigns with a high return on investment (ROI).
- **Banking:** Data analytics can help track and monitor illegal money laundering.

INTERNET OF THINGS

The Internet of Things (IoT) is a concept that refers to the interconnection of everyday physical objects or "things" to the internet or other communication networks. These things can include a wide range of devices and objects, from household appliances and industrial machinery to vehicles and wearable gadgets. The central idea behind IoT is to enable these objects to collect and exchange data, often without requiring direct human intervention. This data exchange enables the objects to be remotely monitored, controlled, and interacted with, which can lead to various applications and benefits.

Why is IoT important?

- **Efficiency and Automation:** IoT enables the automation of various processes, making them more efficient and reliable. This can lead to cost savings, increased productivity, and reduced human intervention in repetitive tasks. For example, in manufacturing, IoT can optimize production processes, and in agriculture, it can improve irrigation and crop management.
- **Data Collection and Insights:** IoT devices collect vast amounts of data from sensors and devices. This data can be analyzed to gain valuable insights and inform decision-

making. Businesses and organizations can use this data to make informed choices, improve operations, and enhance customer experiences.

- **Improved Quality of Life:** In the realm of smart homes, IoT technology enhances the quality of life by providing convenience, energy savings, and security. Smart thermostats, lighting, and security systems are examples of IoT applications that make daily life more comfortable and efficient.
- **Healthcare and Well-being:** IoT has the potential to revolutionize healthcare. Wearable devices, remote patient monitoring, and smart medical equipment can help individuals monitor their health and allow healthcare providers to offer more personalized and timely care.
- **Environmental Sustainability:** IoT can be applied to environmental monitoring and resource management. For instance, it can be used to track air quality, optimize energy usage, and reduce water waste in agriculture.
- **Smart Cities:** IoT is used to create smart cities by improving urban infrastructure and services. Smart traffic management, waste collection, and public transportation systems can enhance the quality of life for city residents and reduce environmental impact.
- **Safety and Security:** IoT can enhance safety and security in various contexts. This includes applications such as home security systems, industrial safety monitoring, and emergency response systems that can be more efficient and effective with IoT technology.
- **Supply Chain and Logistics:** IoT improves supply chain management by enabling real-time tracking of goods and assets. This reduces losses, enhances transparency, and streamlines logistics operations.
- **Health and Safety Monitoring:** In industrial settings, IoT can monitor the health and safety of workers, ensuring that they are operating in a safe environment and promptly responding to any potential risks or incidents.
- **Innovation and Economic Growth:** IoT fosters innovation in product development and service delivery, creating new business opportunities and driving economic growth. It encourages entrepreneurship and job creation in technology-related fields.
- **Competitiveness:** Companies and organizations that adopt IoT can gain a competitive edge by offering innovative products and services, improving customer experiences, and optimizing their operations.
- **Global Connectivity:** IoT promotes global connectivity, enabling information and data to be shared across borders and facilitating communication and cooperation on a global scale.

The technologies that make IoT possible:

- **Sensors and actuators:** Sensors are devices that can detect changes in the environment, such as temperature, humidity, light, motion or pressure. Actuators are devices that can cause physical changes in the environment, such as opening or closing a valve or turning on a motor. These devices are at the heart of IoT, as they allow machines and devices to interact with the physical world. Automation is possible when sensors and actuators work to resolve issues without human intervention.
- **Connectivity technologies:** To transmit IoT data from sensors and actuators to the cloud, IoT devices need to be connected to the internet. There are several connectivity technologies used in IoT, including Wi-Fi, Bluetooth.....
- **Cloud computing:** The cloud is where the vast amounts of data generated by IoT devices are stored, processed and analyzed. Cloud computing platforms provide the infrastructure and tools needed to store and analyze this data, as well as to build and deploy IoT applications.
- **Big data analytics:** To make sense of the vast amounts of data generated by IoT devices, businesses need to use advanced analytics tools to extract insights and identify patterns. These tools can include machine learning algorithms, data visualization tools and predictive analytics models.
- **Security and privacy technologies:** As IoT deployments become more widespread, IoT security and privacy become increasingly important. Technologies such as encryption, access controls and intrusion detection systems are used to protect IoT devices and the data they generate from cyber threats.

IoT APPLICATION

- **Smart Home:** Home automation systems use IoT to control and monitor household appliances, lighting, thermostats, security cameras, and locks. Users can manage these devices remotely through mobile apps or voice commands.
- **Industrial IoT (IIoT):** IIoT is used in manufacturing and industrial processes to monitor and optimize equipment and processes. It can help improve production efficiency, reduce downtime, and enable predictive maintenance.
- **Smart Cities:** IoT is used to enhance urban infrastructure and services. Applications include smart traffic management, waste management, public transportation, environmental monitoring, and smart street lighting.
- **Healthcare:** IoT devices and wearables can monitor patients' health, collect vital signs, and transmit data to healthcare providers. This enables remote patient monitoring and early intervention.

- **Agriculture:** IoT is used in precision agriculture to monitor soil conditions, weather, and crop health. It helps farmers optimize irrigation, fertilization, and pest control for improved crop yield.

INDUSTRIAL IoT:

Industrial IoT (IIoT) refers to smart devices used in manufacturing, retail, health, and other enterprises to create business efficiencies. Industrial devices, from sensors to equipment, give business owners detailed, real-time data that can be used to improve business processes. They provide insights on supply chain management, logistics, human resource, and production – decreasing costs and increasing revenue streams.

APPLICATION OF IIoT

- **Manufacturing:** Enterprise IoT in manufacturing uses predictive maintenance to reduce unplanned downtime and wearable technology to improve worker safety. IoT applications can predict machine failure before it happens, reducing production downtime. Wearables in helmets and wristbands, as well as computer vision cameras, are used to warn workers about potential hazards.
- **Automobile:** Sensor-driven analytics and robotics increase efficiency in automobile manufacturing and maintenance. For example, industrial sensors are used to provide 3D real-time images of internal vehicle components. Diagnostics and troubleshooting can be done much faster while the IoT system orders replacement parts automatically.
- **Logistics and transport:** Commercial and Industrial IoT devices can help with supply chain management, including inventory management, vendor relationships, fleet management, and scheduled maintenance. Shipping companies use Industrial IoT applications to keep track of assets and optimize fuel consumption on shipping routes. The technology is especially useful for tight temperature control in refrigerated containers. Supply chain managers make informed predictions through smart routing and rerouting algorithms.
- **Retail:** Amazon is driving innovation in automation and human-machine collaboration in retail. Amazon facilities make use of internet-connected robots for tracking, locating, sorting, and moving products.

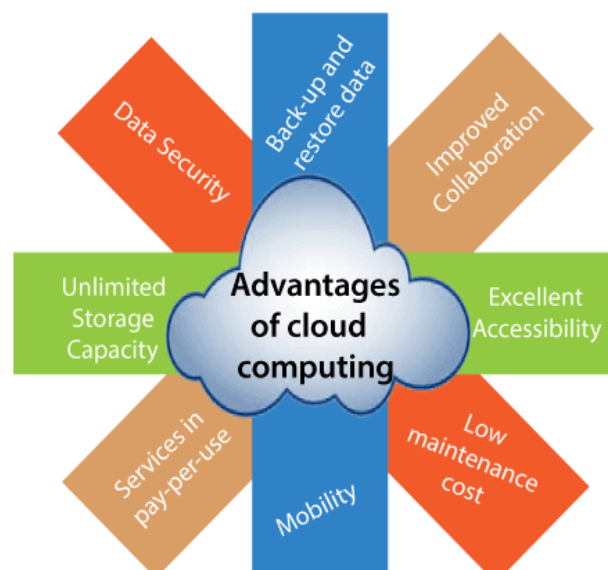
CLOUD COMPUTING AND ITS SERVICE MODELS

Cloud Computing: The term cloud refers to a network or the internet. It is a technology that uses remote servers on the internet to store, manage, and access data online rather than local drives. The data can be anything such as files, images, documents, audio, video, and more.

These are the following operations that can be done using cloud computing:

- Developing new applications and services
- Storage, back up, and recovery of data
- Hosting blogs and websites
- Delivery of software on demand
- Analysis of data
- Streaming videos and audios

ADVANTAGES OF CLOUD COMPUTING



1) Back-up and restore data: **Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud.**

2) Improved collaboration: **Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.**

3) Excellent accessibility: **Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection. An internet cloud infrastructure increases organization productivity and efficiency by ensuring that our data is always accessible.**

4) Low maintenance cost: **Cloud computing reduces both hardware and software maintenance costs for organizations.**

5) Mobility: **Cloud computing allows us to easily access all cloud data via mobile.**

6) Services in the pay-per-use model: **Cloud computing offers Application Programming Interfaces (APIs) to the users for access services on the cloud and pays the charges as per the usage of service.**

7) Unlimited storage capacity: **Cloud offers us a huge amount of storing capacity for storing our important data such as documents, images, audio, video, etc. in one place.**

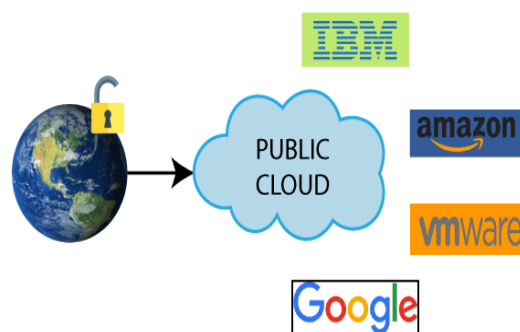
8) Data security: **Data security is one of the biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that data is securely stored and handled.**

SERVICE MODELS:

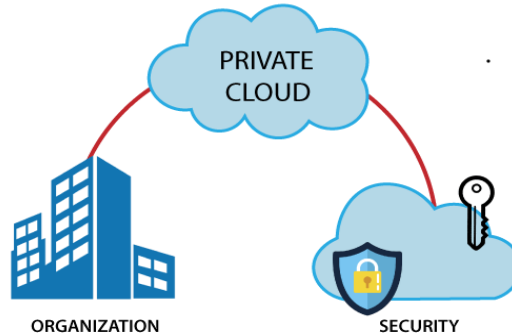
- **Infrastructure as a Service (IaaS):** Provides virtualized computing resources over the internet. Users can rent virtual machines, storage, and networking components.
- **Platform as a Service (PaaS):** Offers a platform that includes both hardware and software tools for application development. Users can build, deploy, and manage applications without worrying about the underlying infrastructure.
- **Software as a Service (SaaS):** Delivers software applications over the internet on a subscription basis. Users can access the software through a web browser without installing or maintaining it locally.

TYPES OF CLOUD:

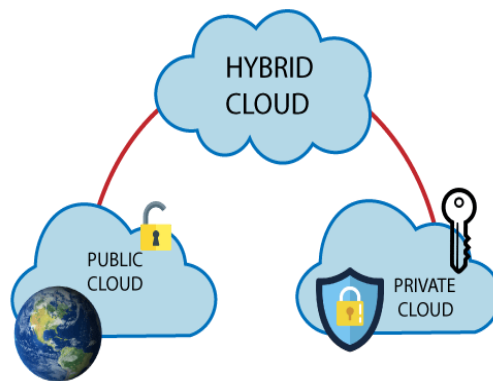
- **Public Cloud:** Public cloud is open to all to store and access information via the Internet using the pay-per-usage method. In public cloud, computing resources are managed and operated by the Cloud Service Provider (CSP). Example: Amazon elastic compute cloud (EC2), IBM SmartCloud Enterprise, Microsoft, Google App Engine, Windows Azure Services Platform.



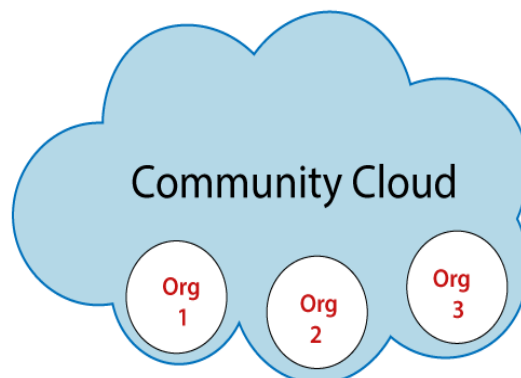
- **Private Cloud:** Private cloud is also known as an internal cloud or corporate cloud. It is used by organizations to build and manage their own data centers internally or by the third party. It can be deployed using Opensource tools such as Openstack and Eucalyptus.



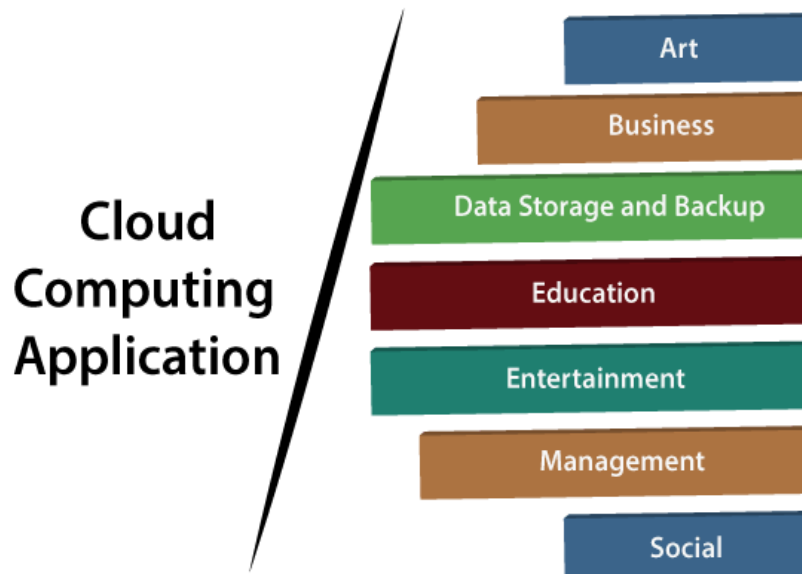
- **Hybrid Cloud:** Hybrid Cloud is a combination of the public cloud and the private cloud.



- **Community Cloud:** Community cloud allows systems and services to be accessible by a group of several organizations to share the information between the organization and a specific community. It is owned, managed, and operated by one or more organizations in the community, a third party, or a combination of them.



APPLICATIONS OF CLOUD COMPUTING



1. Art Applications: Cloud computing offers various art applications for quickly and easily design **attractive cards, booklets, and images**.
2. Business Applications: Business applications are based on cloud service providers. Today, every organization requires the cloud business application to grow their business. It also ensures that business applications are 24*7 available to users.
3. Data Storage and Backup Applications: Cloud computing allows us to store information (data, files, images, audios, and videos) on the cloud and access this information using an internet connection. As the cloud provider is responsible for providing security, so they offer various backup recovery application for retrieving the lost data.
4. Education Applications: Cloud computing in the education sector becomes very popular. It offers various **online distance learning platforms** and **student information portals** to the students. The advantage of using cloud in the field of education is that it offers strong virtual classroom environments, Ease of accessibility, secure data storage, scalability, greater reach for the students, and minimal hardware requirements for the applications.
5. Entertainment Applications: Entertainment industries use a **multi-cloud strategy** to interact with the target audience. Cloud computing offers various entertainment applications such as online games and video conferencing.
6. Management Application: Cloud computing offers various cloud management tools which help admins to manage all types of cloud activities, such as resource deployment, data integration, and disaster recovery. These management tools also provide administrative control over the platforms, applications, and infrastructure.

7. **Social Applications:** Social cloud applications allow a large number of users to connect with each other using social networking applications such as **Facebook, Twitter, LinkedIn**, etc.

CYBER SECURITY

Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies.

TYPES OF CYBER SECURITY

- **Network Security:** Network security involves the protection of computer networks from unauthorized access, attacks, and intrusions. It includes the use of firewalls, VPNs (Virtual Private Networks), intrusion detection and prevention systems, and other technologies to secure data in transit.
- **Endpoint Security:** Endpoint security focuses on securing individual devices such as computers, smartphones, and tablets. This includes antivirus software, endpoint detection and response (EDR), and mobile device management (MDM) solutions to protect against malware, ransomware, and other threats.
- **Application Security:** Application security involves measures taken to secure software applications and the systems they run on. This includes secure coding practices, regular security testing, and the use of web application firewalls (WAFs) to protect against common web-based attacks.
- **Cloud Security:** Cloud security addresses the unique challenges associated with cloud computing environments. It includes measures to secure data, applications, and infrastructure in cloud platforms. Encryption, access controls, and identity management are crucial components of cloud security.
- **Data Security:** Data security focuses on protecting sensitive information from unauthorized access, disclosure, alteration, and destruction. Encryption, access controls, and data loss prevention (DLP) technologies are used to safeguard data.
- **IoT (Internet of Things) security:** IoT security seeks to minimize the vulnerabilities that these proliferating devices bring to organizations. It uses different types of cybersecurity to detect and classify them, segment them to limit network exposure, and seek to mitigate threats related to unpatched firmware and other related flaws.
- **Mobile security:** Mobile security encompasses types of cybersecurity used to protect mobile devices (e.g., phones, tablets, and laptops) from unauthorized access

- **Identity and Access Management (IAM):**
- Identity and Access Management (IAM) is the practice of managing user identities and controlling access to resources within an organization. IAM includes various security measures such as user authentication, authorization, and access control.
- **Security Governance and Compliance:** Security governance involves establishing and maintaining the overall security strategy, policies, and compliance measures within an organization. Compliance efforts ensure that security practices align with relevant laws, regulations, and industry standards.
- **Wireless Security:** Wireless security focuses on securing wireless networks and devices, including Wi-Fi networks and Bluetooth connections. Encryption, strong authentication, and monitoring are essential for protecting wireless communications.
- **Physical Security:** While often overlooked in the digital realm, physical security is crucial for protecting the hardware and infrastructure that house sensitive information. This includes securing data centers, server rooms, and other critical physical locations.

TYPES OF CYBER ATTACK

- **Malware Attack**
 1. This is one of the most common types of cyberattacks. “Malware” refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans.
 2. The trojan virus disguises itself as legitimate software (exporting files, modifying data, deleting files or otherwise altering the contents of the device).
 3. Ransomware blocks access to the network's key components, whereas Spyware is software that steals all your confidential data without your knowledge.
 4. Adware is software that displays advertising content such as banners on a user's screen.
- **Phishing Attack:** Phishing attacks are one of the most prominent widespread types of cyberattacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails. Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By doing so, attackers gain access to confidential information and account credentials.
- **Password Attack:** It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Aircrack, Cain, Abel, John the Ripper, Hashcat, etc. There are different types of password attacks like brute force attacks, dictionary attacks, and keylogger attacks.

- **Man-in-the-Middle Attack:** A Man-in-the-Middle Attack (MITM) is also known as an eavesdropping attack. In this attack, an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data.
- **SQL Injection Attack :** A Structured Query Language (SQL) injection attack occurs on a database-driven website when the hacker manipulates a standard SQL query. It is carried by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information.
- **Denial-of-Service Attack:** A Denial-of-Service Attack is a significant threat to companies. Here, attackers target systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth.
- **Insider Threat:** As the name suggests, an insider threat does not involve a third party but an insider. In such a case; it could be an individual from within the organization who knows everything about the organization. Insider threats have the potential to cause tremendous damages.
- **Zero-Day Exploit:** A Zero-Day Exploit happens after the announcement of a network vulnerability; there is no solution for the vulnerability in most cases. Hence the vendor notifies the vulnerability so that the users are aware; however, this news also reaches the attackers. Depending on the vulnerability, the vendor or the developer could take any amount of time to fix the issue. Meanwhile, the attackers target the disclosed vulnerability. They make sure to exploit the vulnerability even before a patch or solution is implemented for it.

APPLICATIONS OF CYBER SECURITY

Securing AI systems and applications:

- As the adoption of **AI** technologies is increasing, cyber security plays a crucial role in protecting various AI algorithms and models.
- By making use of various encryption techniques, the AI model files that are saved on various systems such as servers, system files, folders, etc. can be protected from getting breached or hacked.

Risk management:

- Risk management and risk analysis are the two main components of the cyber security risk management domain.
- It helps in maintaining data integrity, security, and risk analysis.
- It is made sure that the data is kept secure with the help of data security provided by various available cyber security solutions.

Secured data sharing:

- Cyber security solutions also provide secure file sharing by providing encryption to all the transport layers, especially cloud security.

Defending critical systems:

- Wide-area network connections help avoid attacks on massive systems.
- It upholds rigid safety requirements that are industry-standard for users to follow in order to secure the devices using cybersecurity procedures.
- It continuously monitors all programs and assesses the security of the network, servers, and users.

Network monitoring:

- The practice of continuously scanning a network for signs of dangerous or intrusive behavior is known as network monitoring. It frequently works in collaboration with additional security technologies like firewalls, antivirus programs