Management Information System

Saini Das
Vinod Gupta School of Management, IIT Kharagpur

Module 09: Emerging Technologies
Cloud Computing Part - I

Cloud Computing

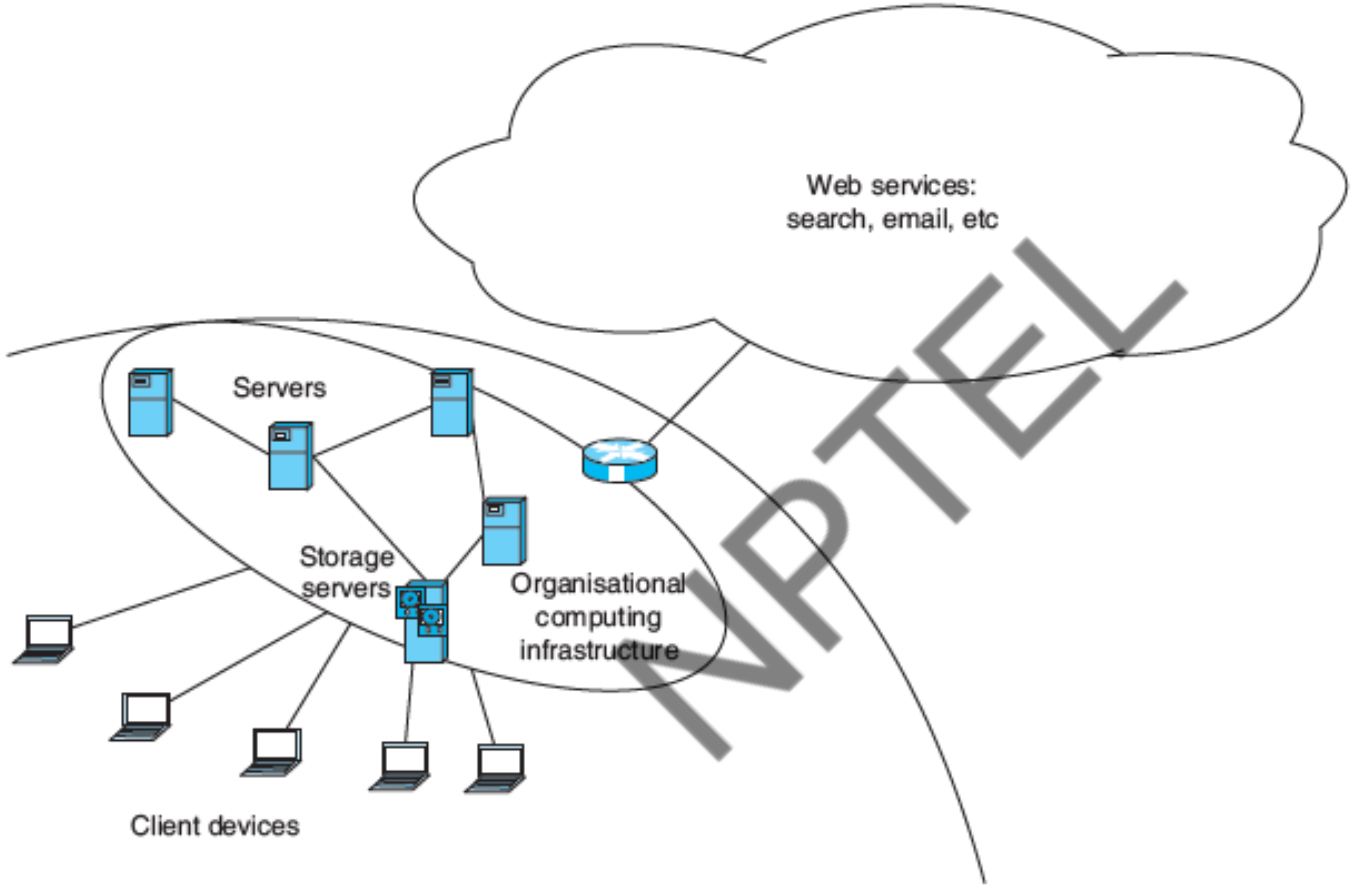
"Cloud computing is cool technology,
but every time it rains I lose my data!"

buzzingup.com

What is Cloud Computing?

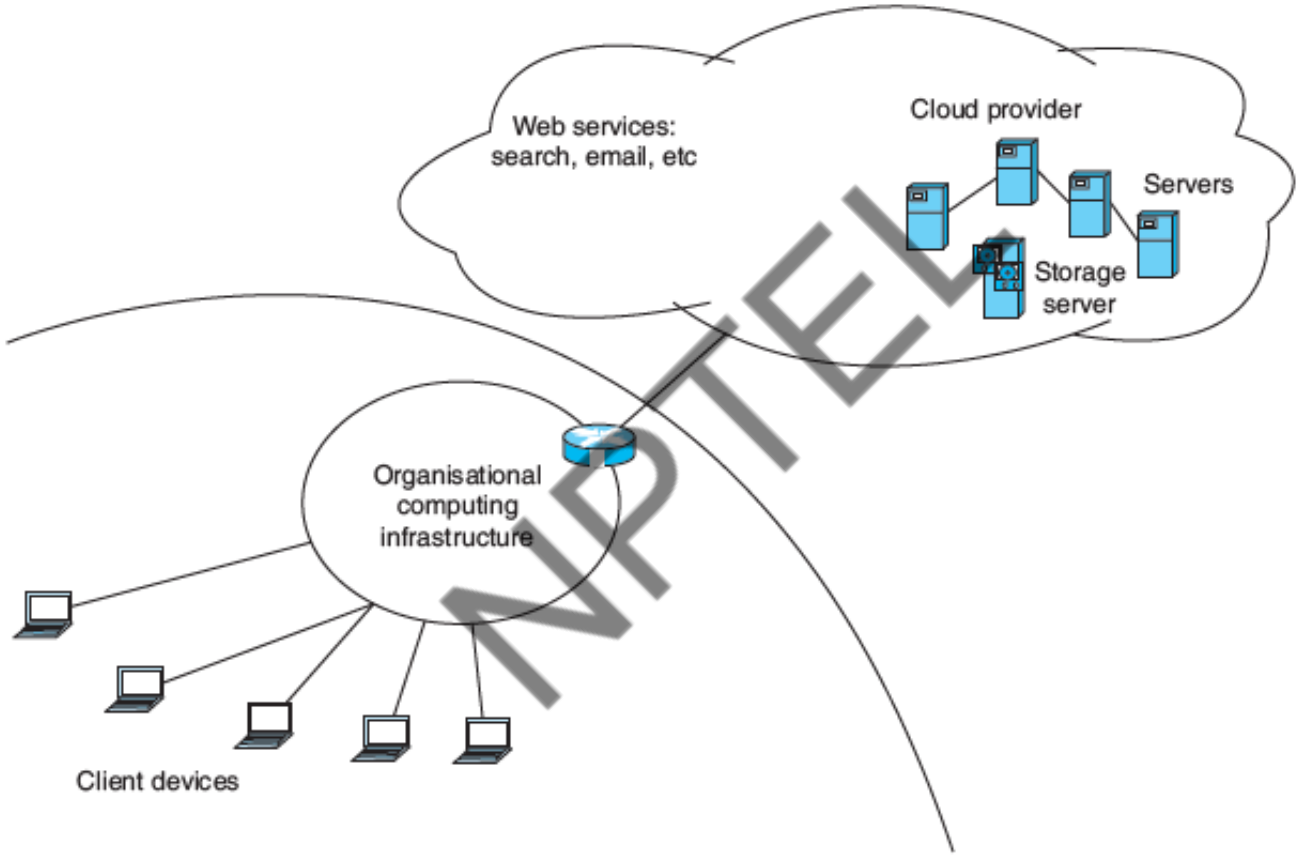
- *"It is an **information technology service model** where computing services (both hardware and software) are delivered **on-demand** to customers over a network in a self-service fashion, independent of device and location. The resources required to provide the requisite quality of service levels are **shared, dynamically scalable, rapidly provisioned and released with minimal client interaction.** Users pay for the service as an **operating expense** without incurring any significant initial **capital expenditure**" (Marston et al., 2012)*

Traditional Computing Architecture



Hosted infrastructure. Here the organisation owns and maintains its own infrastructure of servers and draws on some web-based services from the internet.

Cloud Computing Architecture



Cloud infrastructure: Here an organisation draws on server and storage resources from the cloud and maintains a minimal infrastructure internally.

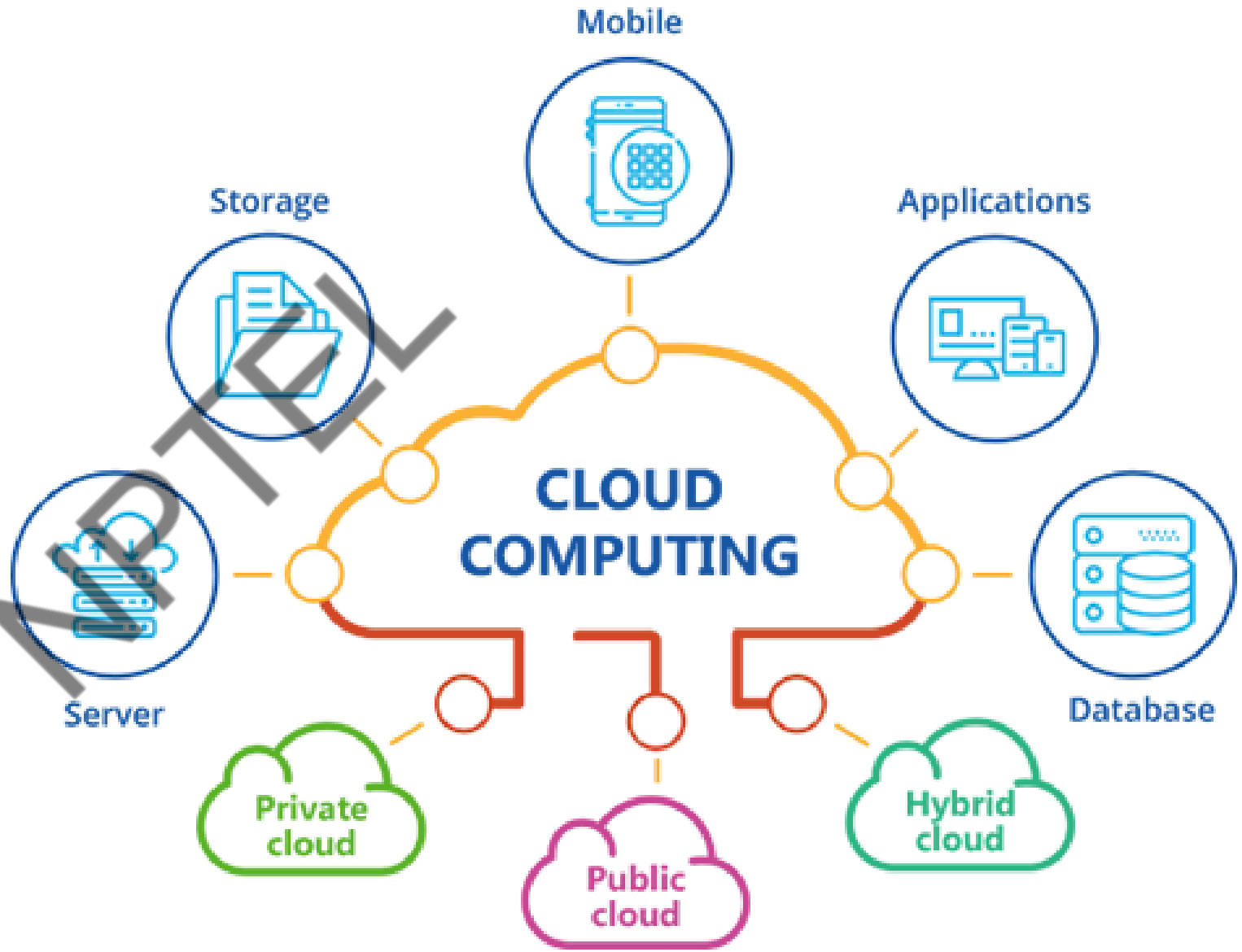
Benefits of Cloud Computing

- Scalability
- Measured Use
  - Memory usage in unit time; CPU utilization in cycles per unit time; data usage in bits per unit time etc.
- Usage-based pricing
- Managed Services
- Service levels
  - Duration of time an infrastructure is available without interruption; speed of a service over a period of time etc.
- Ubiquitous Access
- Reduced Set-up Time
- Resource Pooling

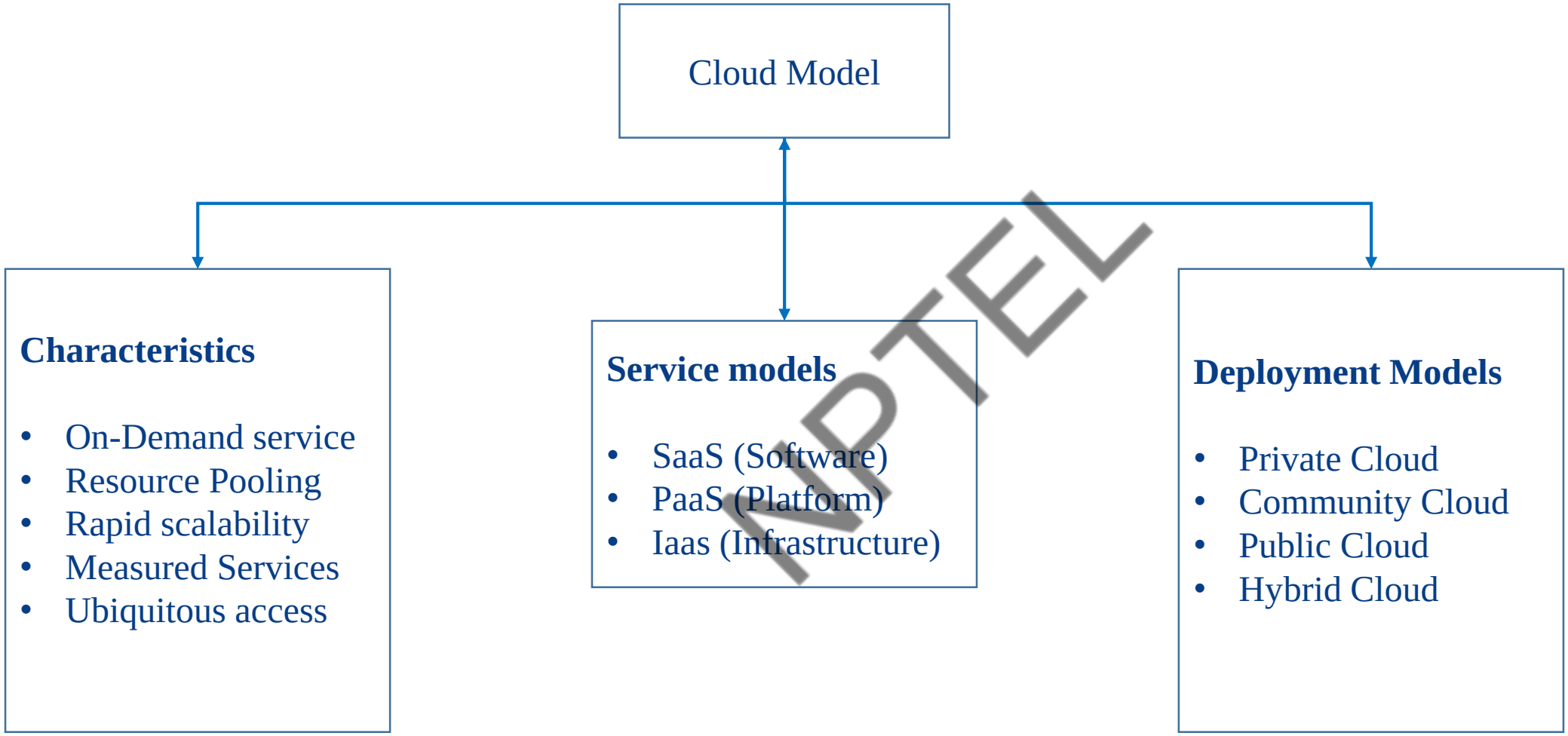
Cloud Service Providers

Top 12 Service Providers

- Amazon Web Services
- Kamatera
- DigtialOcean
- Rackspace
- MassiveGrid
- Alibaba Cloud
- LiquidWeb
- Microsoft Azure
- Google Cloud Platform
- VMware
- Salesforce
- Oracle Cloud



Cloud Model Hierarchy



Cloud Service Models

- **IaaS** : Single server or group of servers, CPU, memory, bunch of storage capacity, networking facilities, security solutions such as firewalls or bandwidth in the cloud. Eg: Amazon web services, Microsoft Azure etc.

- **PaaS** : Cloud-based platform that companies can use to develop their custom applications or write software that integrates with existing applications. The vendor hosts the application development tools, packages, plugins and libraries and makes it widely available. Vendors are Microsoft, Amazon, etc.

- **SaaS** : Application or suite of applications that resides in the cloud instead of on a user's hard drive or in a data center. Most mature.
- Eg: Salesforce.com's CRM software

IaaS provides data centre facilities; PaaS provides a software development facility; SaaS provides applications over the Internet.

Cloud Service Models Comparison

Feature	IaaS	PaaS	SaaS
What is provided	Hardware + System software + Networking software + System management tools	IaaS + Application development tools and libraries	Cloud-based Application
Management	Vendor manages infrastructure; everything else managed by client	Vendor manages infrastructure and development tools; client manages everything else	Vendor manages infrastructure and application; client manages user accounts only
Typical usage	Infrastructure for multiple servers and applications	Build and deploy new applications; maybe for new markets	Single application for focussed use

Challenges

- Security and privacy
- Availability and reliability
- Service quality
- Integration
- Regulations

Cloud Deployment models

- **Public** : Services are rendered over a network that is open for public use. Truly shared facility that allows multiple clients to use the resources provided.
- **Private** : Cloud infrastructure operated solely for a single organization, either managed internally or by a third-party, and hosted either internally or externally.
- **Hybrid** : Cloud computing service that is composed of some combination of private and public cloud services, sometimes from different service providers.
- **Community Cloud**: Shared computing infrastructure set up as a public, private or hybrid cloud used by a specified community of users such as hospitals or banks.

References

- K. Laudon and J. Laudon (2016). Management Information Systems Publisher: Pearson. Edition 14e.

- R. De. (2018). MIS Managing Information Systems in Business, Government and Society. Publisher: Wiley. Second Edition.

Management Information System

Saini Das
Vinod Gupta School of Management, IIT Kharagpur

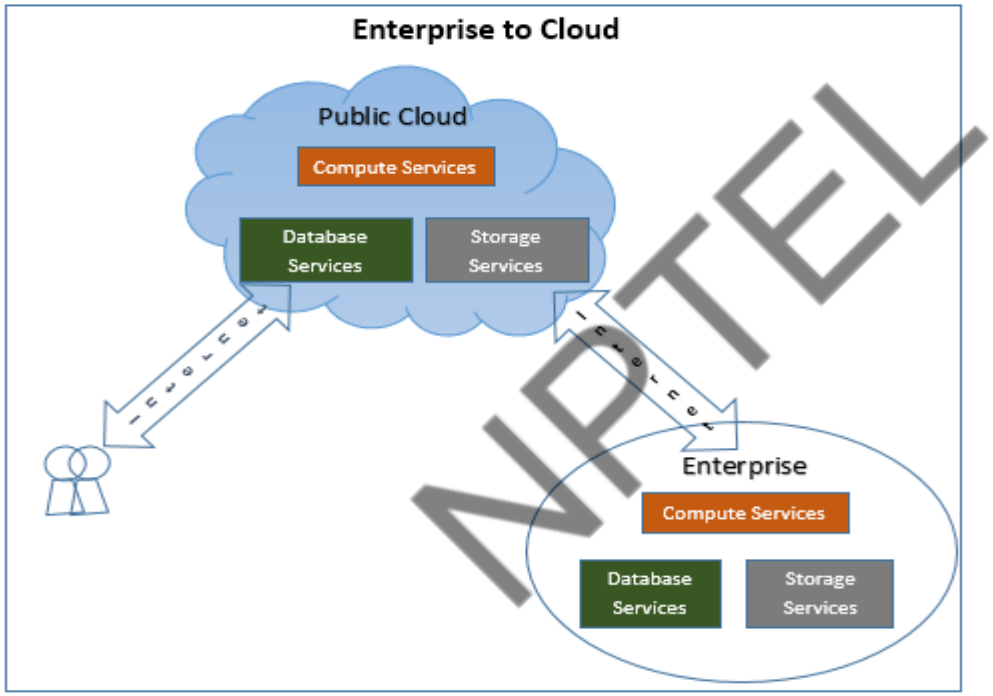
Module 09: Emerging Technologies
Cloud Computing – Part II

Cloud Deployment models

- **Public** : Services are rendered over a network that is open for public use. Truly shared facility that allows multiple clients to use the resources provided.
- **Private** : Cloud infrastructure operated solely for a single organization, either managed internally or by a third-party, and hosted either internally or externally.
- **Hybrid** : Cloud computing service that is composed of some combination of private and public cloud services, sometimes from different service providers.
- **Community Cloud**: Shared computing infrastructure set up as a public, private or hybrid cloud used by a specified community of users such as hospitals or banks.

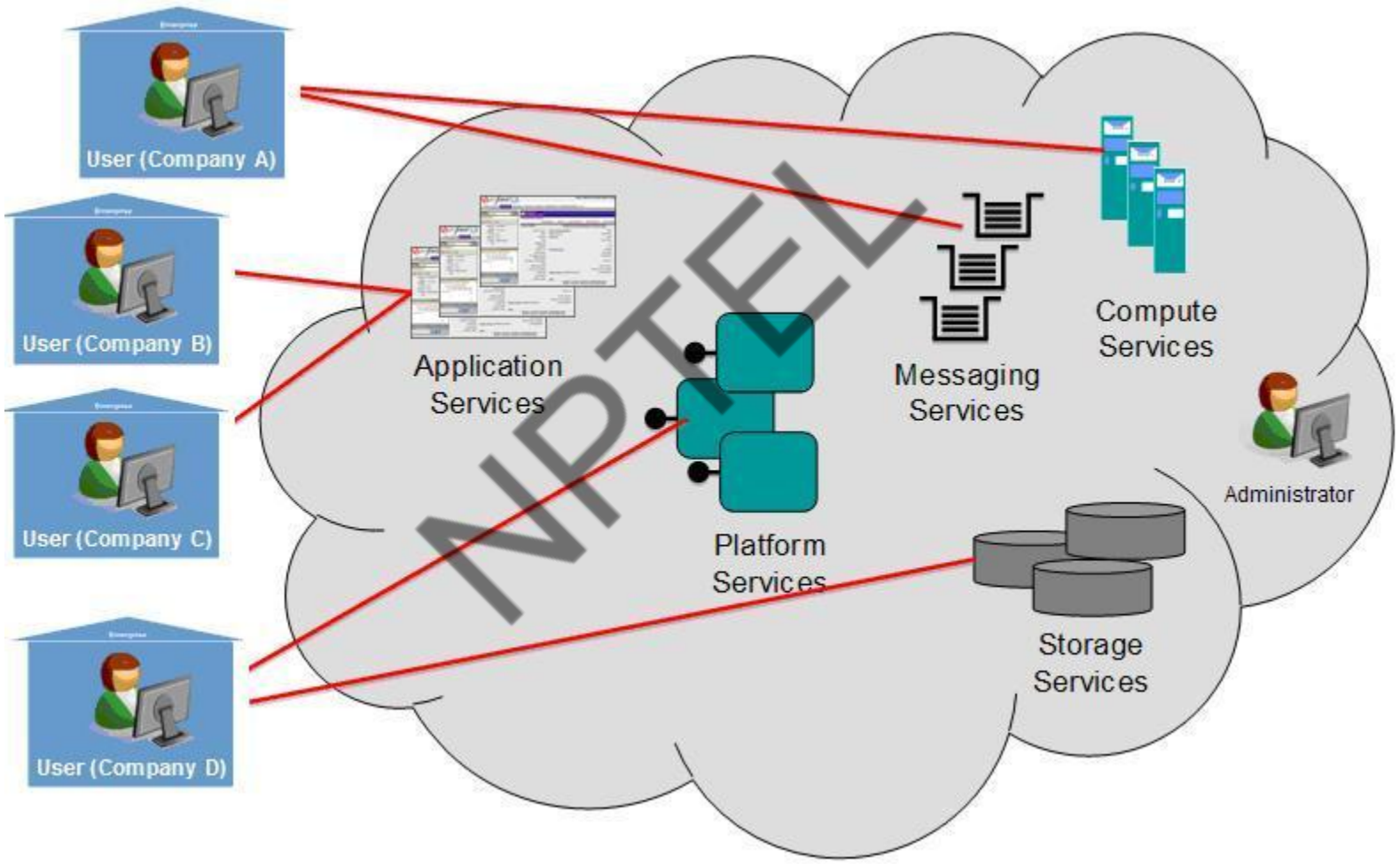
Public Cloud

- Cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.



- In Public setting, the provider's computing and storage resources are potentially large; the communication links can be assumed to be implemented over the public internet; and the cloud serves a diverse pool of clients (and possibly attackers).

Public Cloud (contd..)



Advantages of Public Cloud

- Low up-front costs to migrate to the cloud
- Reduced set-up time
- Cheaper compared to private cloud; pay-per-use
- Scalable; unlimited resources available on demand

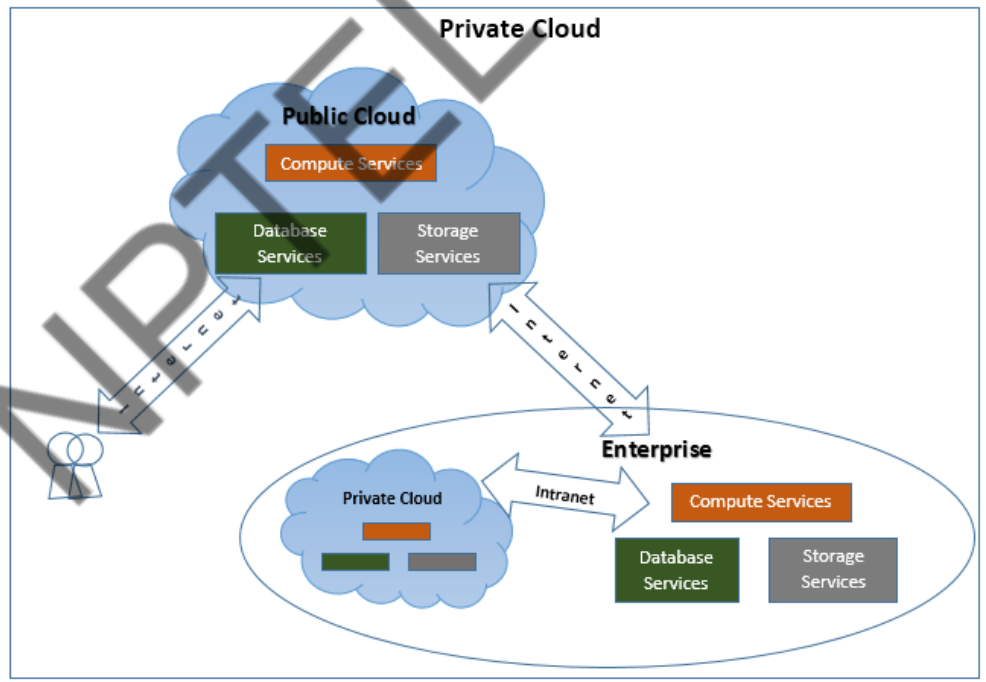
Disadvantages of Public Cloud

- Workload locations are hidden from clients:
  - A provider may migrate a subscriber's workload, whether processing or data, anywhere at any time depending on cost and regulatory restrictions unless the provider has offered (optional) location restriction polices.
- Risks from multi-tenancy:
  - A single machine may be shared with the workloads of competitors or adversaries.
  - Introduces both reliability and security risk.
- Restrictive default service level agreements :
  - The default service level agreements of public clouds specify limited promises that providers make to subscribers
- Limited visibility and control over data regarding security :
  - The details of provider’s system operation and software are usually considered proprietary information and are not divulged to subscribers.
  - Subscribers cannot verify if data has been completely deleted from a provider's systems.

Private Cloud

- The Cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

- Examples of Private Cloud:
  - Eucalyptus
  - Ubuntu Enterprise Cloud- UEC
  - Amazon VPC (Virtual Private Cloud)
  - VMware Cloud Infrastructure Suite
  - Microsoft ECI data center.



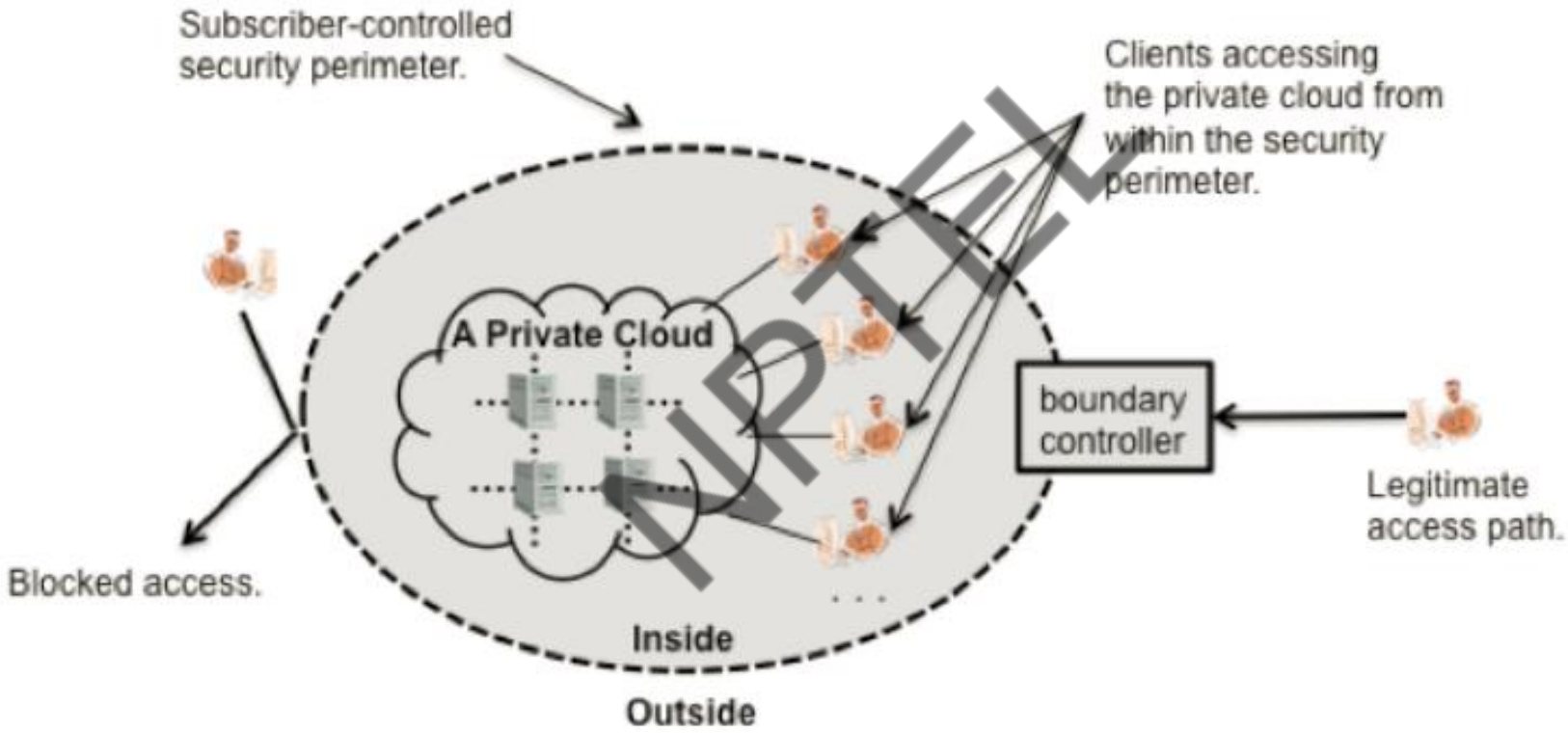
Private Cloud (contd..)

- Contrary to popular belief, private cloud may exist off premises and can be managed by a third party. Thus, two private cloud scenarios exist, as follows:

- On-site Private Cloud
  - Applies to private clouds implemented at a customer's premises.

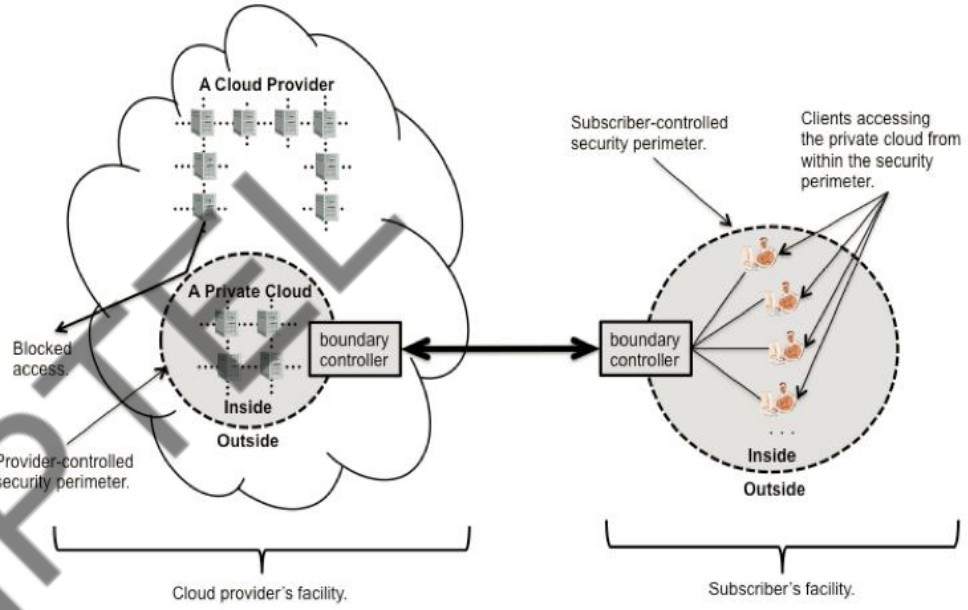
- Outsourced Private Cloud
  - Applies to private clouds where the server side is outsourced to a hosting company.

On-site Private Cloud



Outsourced Private Cloud

- Outsourced private cloud has two security perimeters, one implemented by a cloud subscriber (on the right) and one implemented by a provider.
- Two security perimeters are joined by a protected communication link.
- The security of data and processing depends on the strength and availability of both security perimeters and of protected communication link.



Advantages of Private Cloud

- Potentially strong security from external threats (both on-site and outsourced private)

Disadvantages of Private Cloud

- Subscribers require IT skills (on-site private)
- Significant-to-high up-front costs to migrate into the cloud (on-site-private).
- Network dependency (on-site-private).
- Modest-to-significant up-front costs to migrate into the cloud (outsourced-private).

Community Cloud

- Cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Examples: Microsoft Government Community Cloud
Open Cirrus

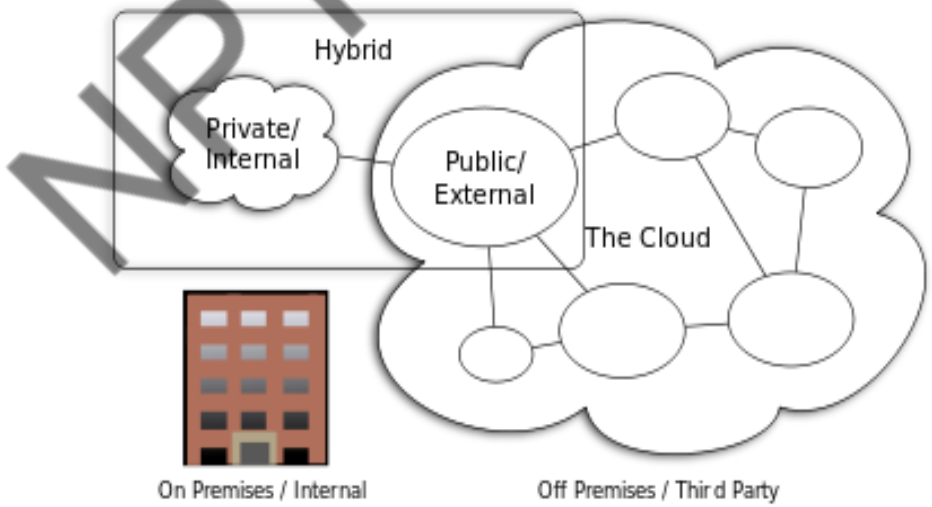
On-site Community Cloud

- Community cloud is made of a set of participant organization. Each participant organization may provide cloud services, consumes cloud services, or both
- At least one organization must provide cloud services
- Each organization implements a security perimeter

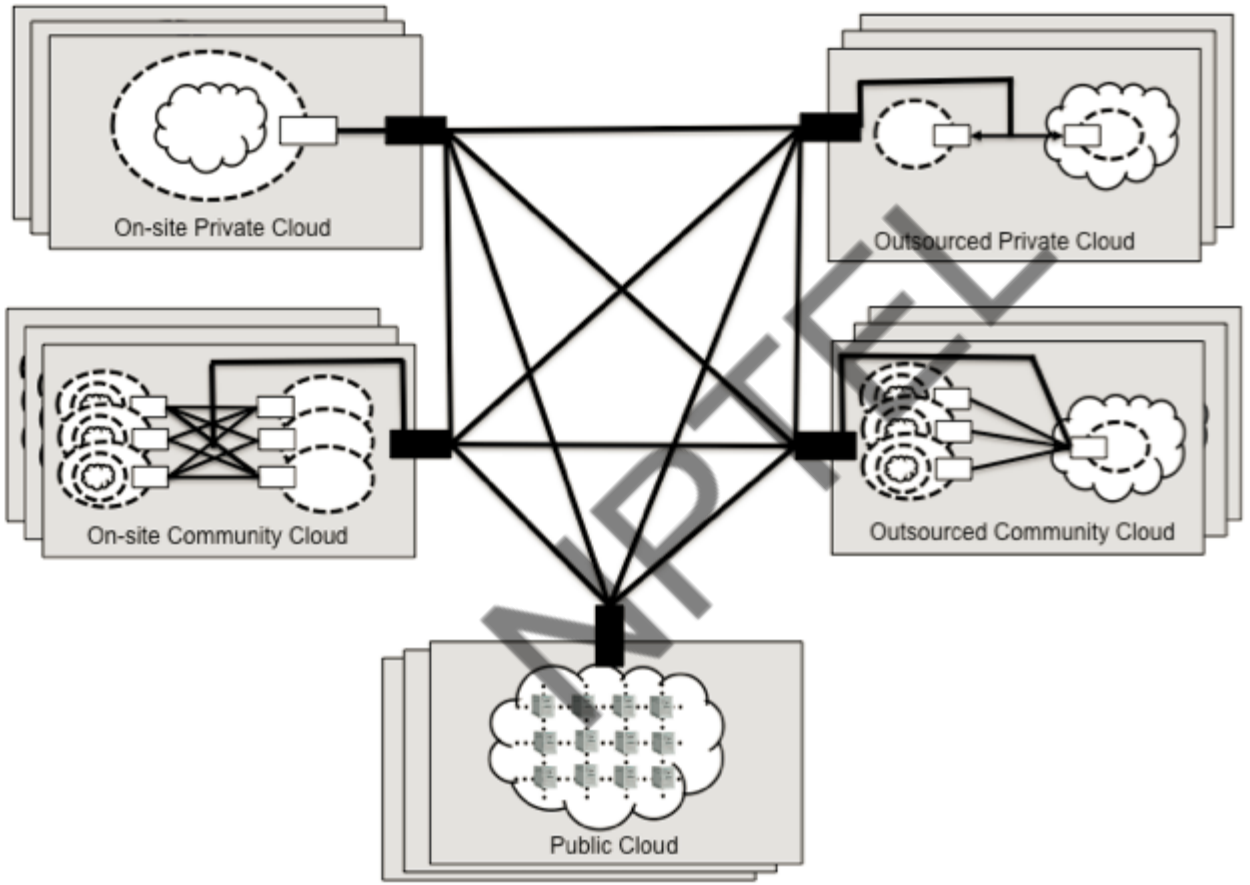
Outsourced Community Cloud

Hybrid Cloud

- A hybrid cloud is a composition of two or more clouds where each constituent cloud is one of the five variants. Hybrid clouds may change over time with constituent clouds joining and leaving.
- Examples:
  - Microsoft Azure (capable of hybrid cloud)
  - VMware vCloud



Hybrid Cloud (contd..)



Examples of hybrid cloud usage

- An e-commerce site relies on Salesforce in the public cloud to manage its customer relationship management (CRM) functions while also using a private cloud to test and build new analytics products based on that data.

- A parts manufacturer relies on a private cloud to collect and analyse billions of points of data coming in from IoT sensors but also needs to enable customers on the public cloud to see real-time order-status updates that depend on that sensor data.

- A major health care provider needs the ability to compartmentalize patient data in compliance with HIPAA through a private cloud while also enabling patients the ability to access some of their information through the provider's web app on a public cloud.

- A defence research organization performs mission-critical defence research using a private cloud but also uses a public cloud for enabling its day-to-day operational matters.

Advantages and Disadvantages of Hybrid Cloud

- Advantages:
  - IT manpower rationalization
  - Adequate amount of security
  - Flexibility
  - Cloud bursting is possible
  - Cost rationalization

- Disadvantages:
  - Complex to manage and handle
  - Volatile

Which Cloud Deployment Model to Choose?

- Spending power
- Security
- Reliability
- In-house IT expertise
- Possibility of cloud bursts
- Flexibility
- Urgency to deploy

References

- K. Laudon and J. Laudon (2016). Management Information Systems Publisher: Pearson. Edition 14e.

- R. De. (2018). MIS Managing Information Systems in Business, Government and Society. Publisher: Wiley. Second Edition.

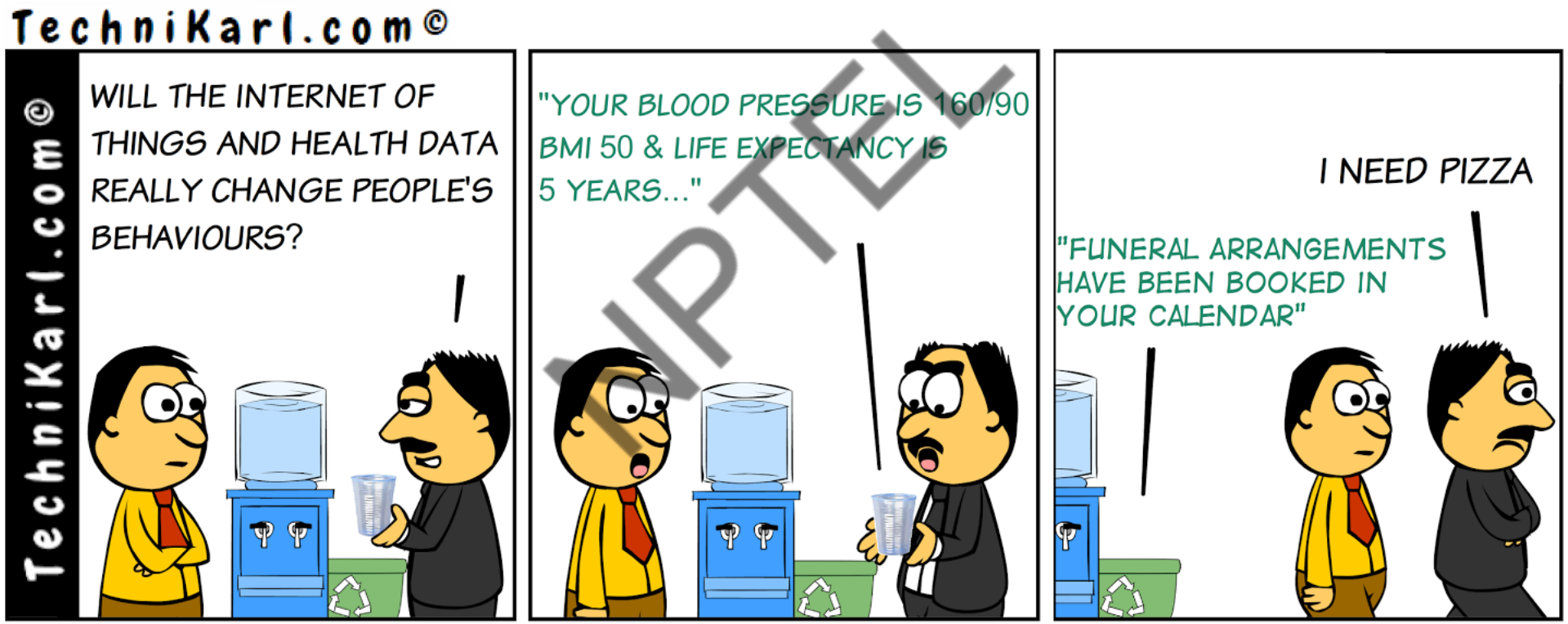
- L. Badger, T. Grance, R. Patt-Corner & J. Voas. (2012). NIST Special Publication 800-146. Cloud Computing Synopsis and Recommendations available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf.

Management Information System

Saini Das
Vinod Gupta School of Management, IIT Kharagpur

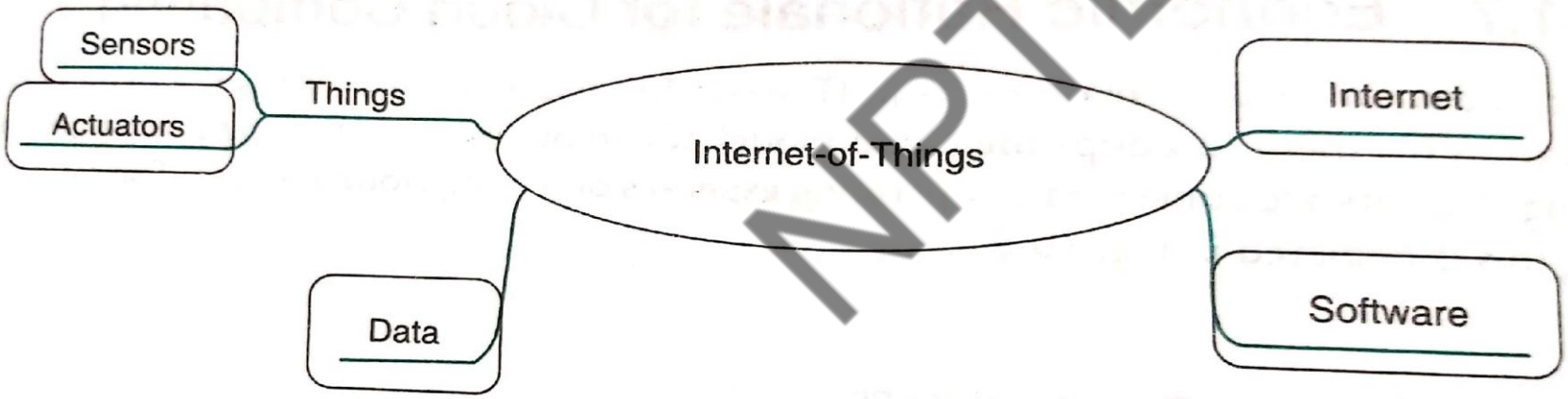
Module 09: Emerging Technologies
Internet of Things Part - I

Internet of Things



What is IoT?

- IoT consists of a large number of devices that are connected via the Internet to sense and respond to conditions in their environments. These devices are typically **sensors** and **actuators** that exchange information with a controlling software for a defined purpose.



Sensors

- A sensor is a device that detects events or changes in its physical environment and provides an electronic output.
    - Simple sensor
    - Smart sensor

- Selection of sensor depends on attributes such as :
    - data filter capacity
    - power consumption
    - size
    - sensitivity and accuracy.

Types of Sensors

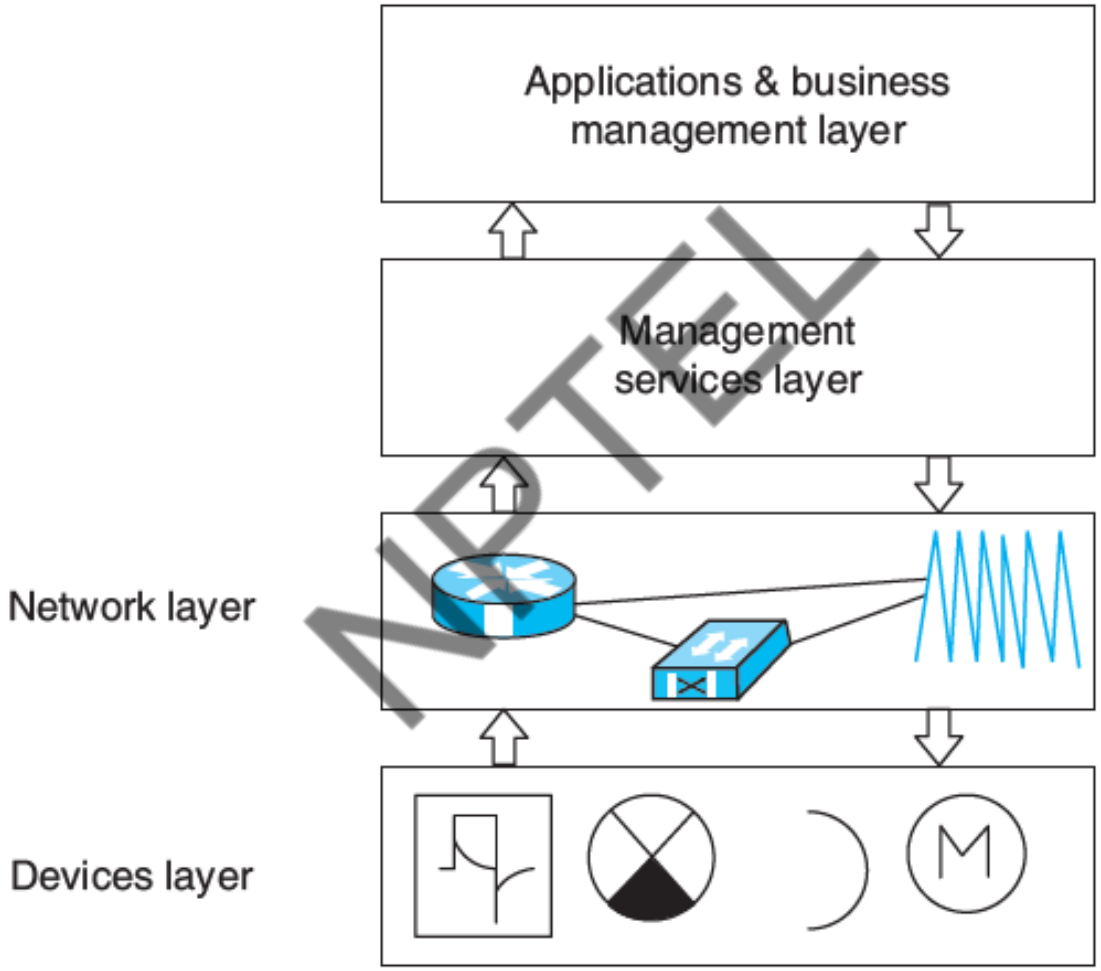
Type of Sensor	Usage
Temperature sensor	Detects changes in temperature or absolute temperature values. Wide applications in industrial machines for chemical and mechanical processes and in biological applications.
Pressure sensor	Measures the pressure of gases or liquids. Is used to measure the levels, flows and altitudes. Also used in touchscreen devices.
Flow sensor	Is used to record the rate of fluid and gas flow in pipes.
Level sensor	Is used to measure the level of liquids in containers.
Image sensor	Records images, including details of colour, intensity and brightness, for devices such as cameras.
Noise sensor	Monitors level and intensity of ambient noise. Is used to gauge noise pollution.
Air particle sensor	Monitors the level of air particles and gases such as carbon dioxide and other pollutants.
Proximity sensor	Detects the presence or absence of objects in the vicinity.
Moisture sensor	Measures the relative humidity of air. Is used inside buildings and factories.
Speed sensors	Measures the speed of objects, such as vehicles.

Actuators

- Actuators are tools or mechanisms that can change their own state and or the state of other devices and machines.
- They are often motors that respond to electrical or data signals and change the state of something they are connected to.

Actuator Type	Usage
Electrical	Motors that convert electrical signals to mechanical motion, e.g., change the position of a valve.
Mechanical	Devices that convert motion or energy into a different movement, e.g., movement of gears or levers.
Hydraulic and Pneumatic	Devices that respond to pressure in liquids and gases, e.g., convert pressure in liquids into pressure on container walls.

IoT Architecture



Four layers of the IoT architecture.

IoT in Smart Cities

- In the context of smart cities there may be sensors in the water infrastructure that sense and collect information on water pressure and water flows.
- This information would be relayed over Internet to a software that would identify the location of the information and process it to determine if any action needs to be taken.
- In case some action is required information will be sent over Internet to the actuators that can effect the changes in pressure and flow of water. For example: Actuator may be a motor that responds to an electronic signal to open, close or change the position of a valve.
- https://www.youtube.com/watch?v=uEsKZGOxNKw

IoT in Residential Water Supply

- Residential water supply is a problem in many parts of the city of Bangalore.
- Due to inadequate water supply households rely either on groundwater that is pumped up to their overhead tanks or purchase water commercially.
- Residents face problem of knowing exactly how much water they have in their storage tanks, on the basis of which they can start or stop motors or place order for water tankers.
- Gnarus Solutions has developed an loT system that addresses this problem.

IoT in Residential Water Supply (contd..)

- They placed sensor devices in water storage tanks in buildings that sensed the water level and sent out the data over a wifi gateway to a controlling software.
- The software processed the data and sent out updates about the water level to an app that could be accessed from the user's smart phone.
- The software also analyzed the data to produce reports on weekly and monthly water consumption patterns.
- The app has additional features that can be used to alert plumbers, tank cleaners or electricians if potential problems arise and users want something fixed or their tanks cleaned.

Healthcare with IoT

- Healthcare devices such as wrist bands and health bands measure body parameters such as heart rate, BP and oxygen levels.

- These parameters are relayed using Bluetooth wireless protocol, to smartphones that forward them to controlling applications.

- The Giraff project in Sweden uses a telepresence robot that is placed in the homes of patients who need monitoring and round-the-clock healthcare support. It promotes “digital aging” at home.

References

- K. Laudon and J. Laudon (2016). Management Information Systems Publisher: Pearson. Edition 14e.

- R. De. (2018). MIS Managing Information Systems in Business, Government and Society. Publisher: Wiley. Second Edition.

Management Information System

Saini Das
Vinod Gupta School of Management, IIT Kharagpur

Module 09: Emerging Technologies
Internet of Things Part - II

Classifying IOT devices by application

- **Wearables**

- Entertainment
- Fitness
- Smart watch
- Location and tracking

- **Building and Home Automation**

- Access control
- Light and temperature control
- Energy optimization
- Predictive maintenance
- Connected appliances

Health Care

- Remote monitoring
- Ambulance telemetry
- Drug tracking
- Hospital asset tracking
- Access control
- Predictive maintenance

Smart Manufacturing

- Flow optimization
- Real-time inventory
- Asset tracking
- Employee safety
- Predictive Maintenance

Classifying IOT devices by application (contd..)

- **Smart Cities**

- Residential e-meters
- Smart street lights
- Pipeline leak detection
- Traffic control
- Surveillance cameras
- Centralized and integrated system control

Automotive

- Infotainment
- Wire replacement
- Predictive Maintenance
- Telemetry

https://www.youtube.com/watch?v=NjYTzvAVozo

IoT Ecosystem

The Internet of Things **ecosystem** includes all the components and players that enable businesses, governments, and consumers to connect to their **IoT** devices. The **ecosystem** includes core, i.e., hardware, software, connectivity, standards, and application services, supporting services.

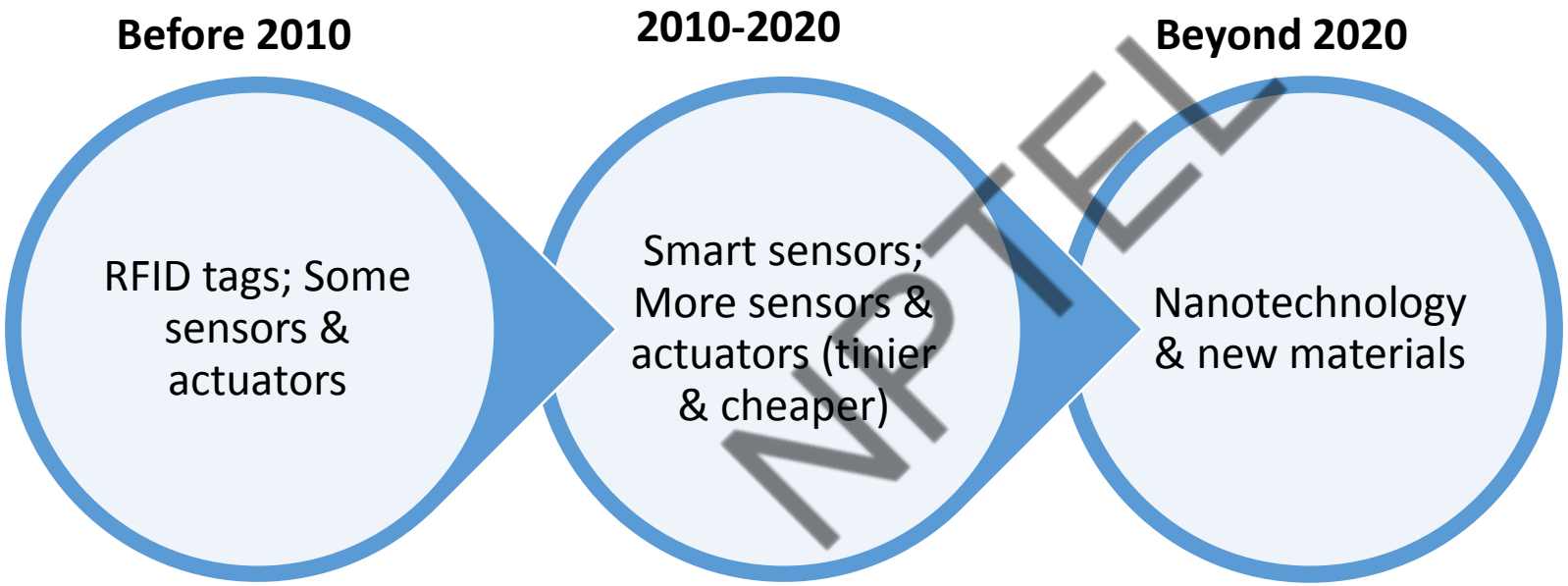
Roles include:

- Chip manufacturer,
- SIM provider,
- Module provider,
- Network operator,
- Network equipment provider
- M2M service provider
- Integrator
- Sensor and actuation service broker
- (App) Developer
- User
- Standard development org. (SDO)
- Regulatory body etc.

Key IoT Technologies

- Hardware
- Software & Algorithms
- Network
- Data processing
- Data storage

Hardware (Things)



IoT >>>>> IoNT

Software & Algorithms

- Objects rely on software to communicate effectively with each other and to deliver enhanced functionality and connectivity.
- The focus of software development is shifting to user-oriented, distributed intelligence and machine-to-machine and machine-to-human collaboration. The evolution of IoT software is as follows:

- IoT oriented Relational DBMS (pre 2010)

- Sensor middleware (2010-2020)

- Goal & User-oriented, easy-to-deploy IoT software (beyond 2020)

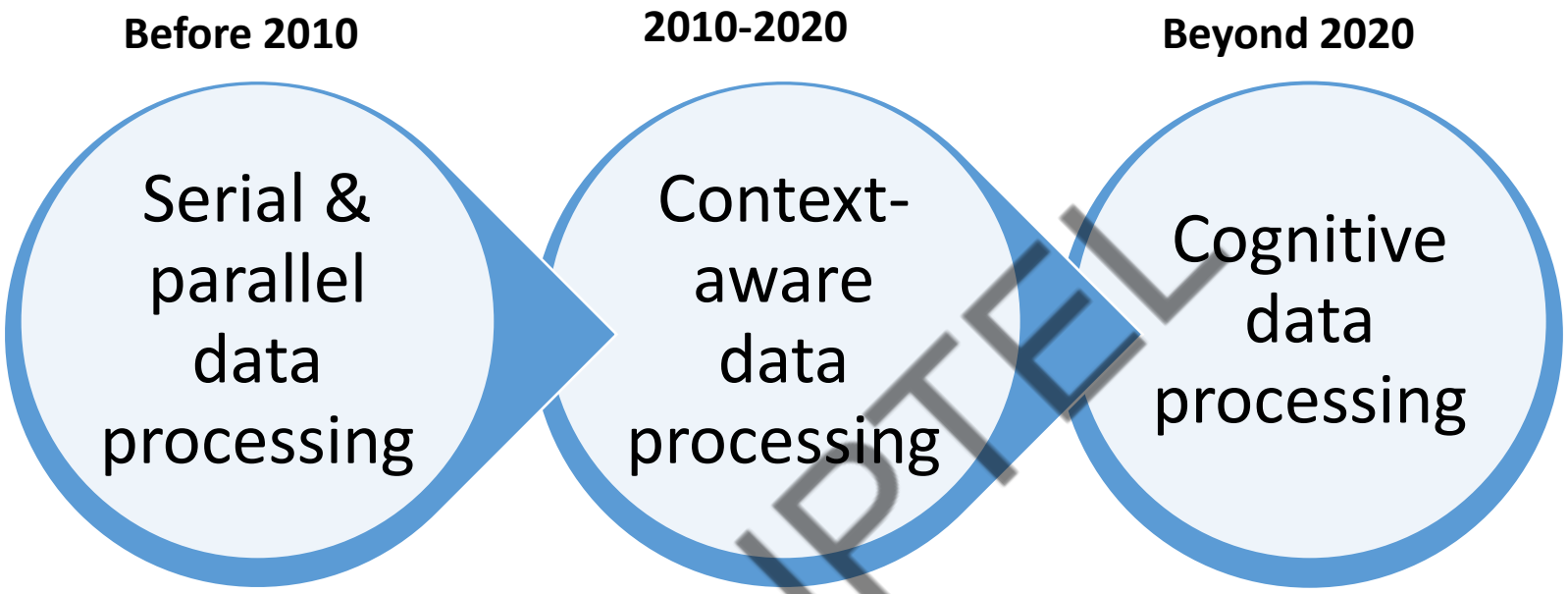
Network Technologies

- Network is the backbone of the IoT environment.
- Over the years network technology is moving to unobtrusive wire-free communication that allows more flexible device-to-device application deployment. The evolution is as follows:

- Sensor Network (pre 2010)

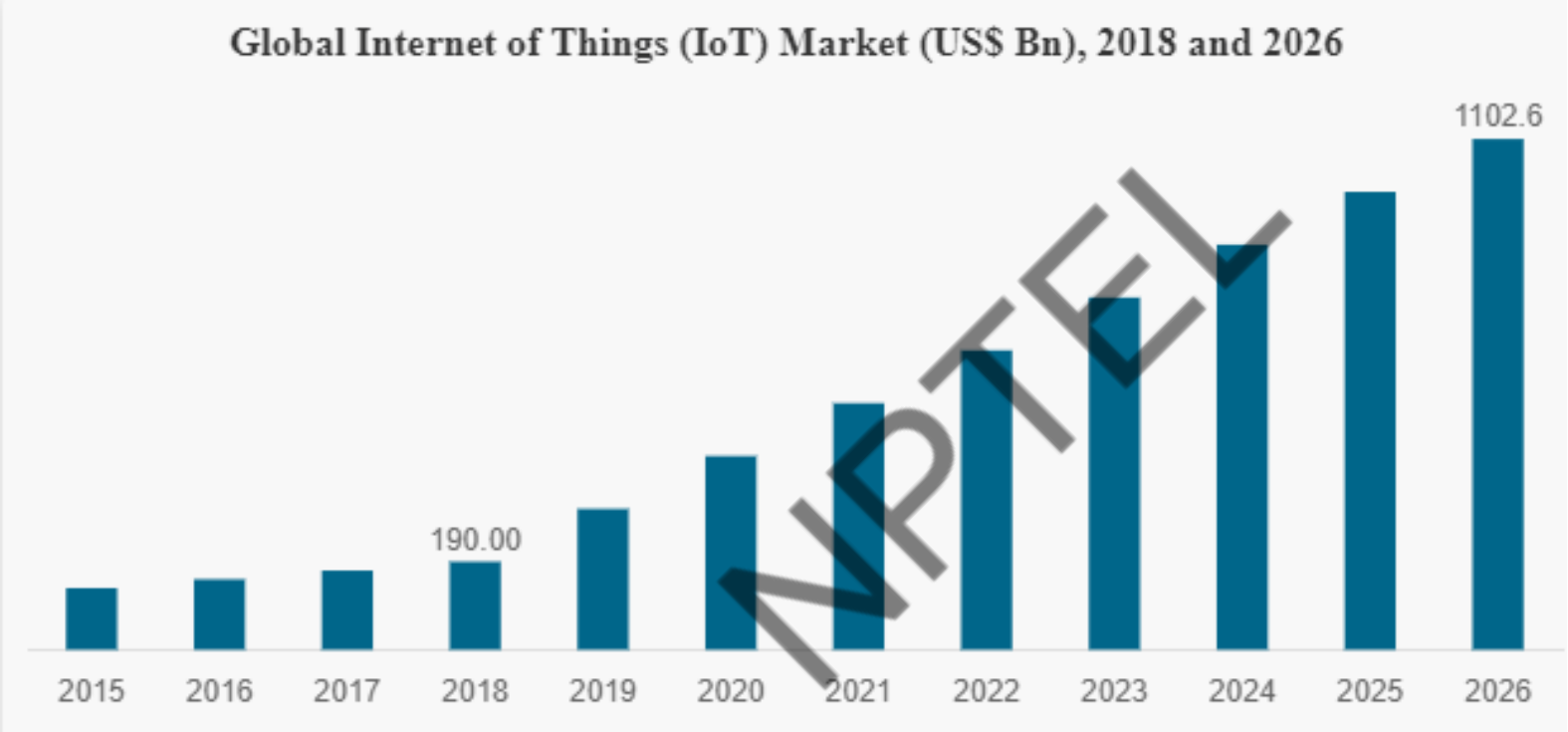
- Autonomous self- organizing & self-repairing network (2010 onward).

Data Processing



- **Context-aware data processing** enables sensors and devices to deliver relevant information to a user based on context-specific data such as users current location, climate and physical conditions (eg: within a home, dept. store, park or museum).
- **Cognitive data processing** optimizes data processing by using AI & machine learning to sense, predict, infer and learn tasks and environment based on user feedback.
- https://www.youtube.com/watch?v=LVlT4sX6uVs

IoT Markets



CAGR of 24.7% in the forecast period

Benefits

- Enhances data collection
- Real-time monitoring and decision-making
    - A CMO could view a dashboard that shows real-time traffic flow patterns within a retail outlet, and have control of in-store elements, such as display monitors, audio, lighting, and shelf stocking.
    - Smart Cities
- Greater access and control of Internet-connected devices
- Increasing efficiency and productivity
    - RFID tags on a variety of manufacturing materials to provide real-time information to assembly workers, supervisors, and managers.Connecting technologies
- Connected technologies
    - Homeowners could have a system where a variety of property-related elements—such as lighting, locks, televisions, and kitchen appliances—could be tied together into a ‘connected’ home.

References

- R. De. (2018). MIS Managing Information Systems in Business, Government and Society. Publisher: Wiley. Second Edition.

- I. Lee & K. Lee. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons.* 58, pp. 431-440.

- B. Weinberg, G. Milne, Y. Andonova, & F. Hajjat. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons.* 58, pp.615-624.

Management Information System

Saini Das
Vinod Gupta School of Management, IIT Kharagpur

Module 09: Emerging Technologies
Internet of Things Part - III

Benefits

- Enhances data collection
- Real-time monitoring and decision-making
    - A CMO views a dashboard that shows real-time traffic flow patterns within a retail outlet and controls in-store elements, such as audio, lighting, and shelf stocking.
    - Smart Cities
    - Healthcare
- Greater access and control of Internet-connected devices
- Increasing efficiency and productivity
    - RFID tags on a variety of manufacturing materials provide real-time information to assembly workers, supervisors, and managers.
- Connected technologies
    - Homeowners could have a system where a variety of elements—such as lighting, locks, televisions, and kitchen appliances—could be tied together into a ‘connected’ home.

Challenges in IoT

- Data Management: Storage and processing of zettabytes of data
- Data Ownership
- Data mining sophistication
  - In 2015 McKinsey Global Institute estimated that the United States needs 140,000 to 190,000 more workers with analytical skills and 1.5 million managers and analysts with analytical skills to make business decisions based on the analysis of big data.
- Privacy and Security
- Legal
- Chaos
- Internet Access

Privacy Challenges of IoT

"The right to be left alone and the right to be free of unreasonable personal intrusions, surveillance or interference from other individuals or organizations".

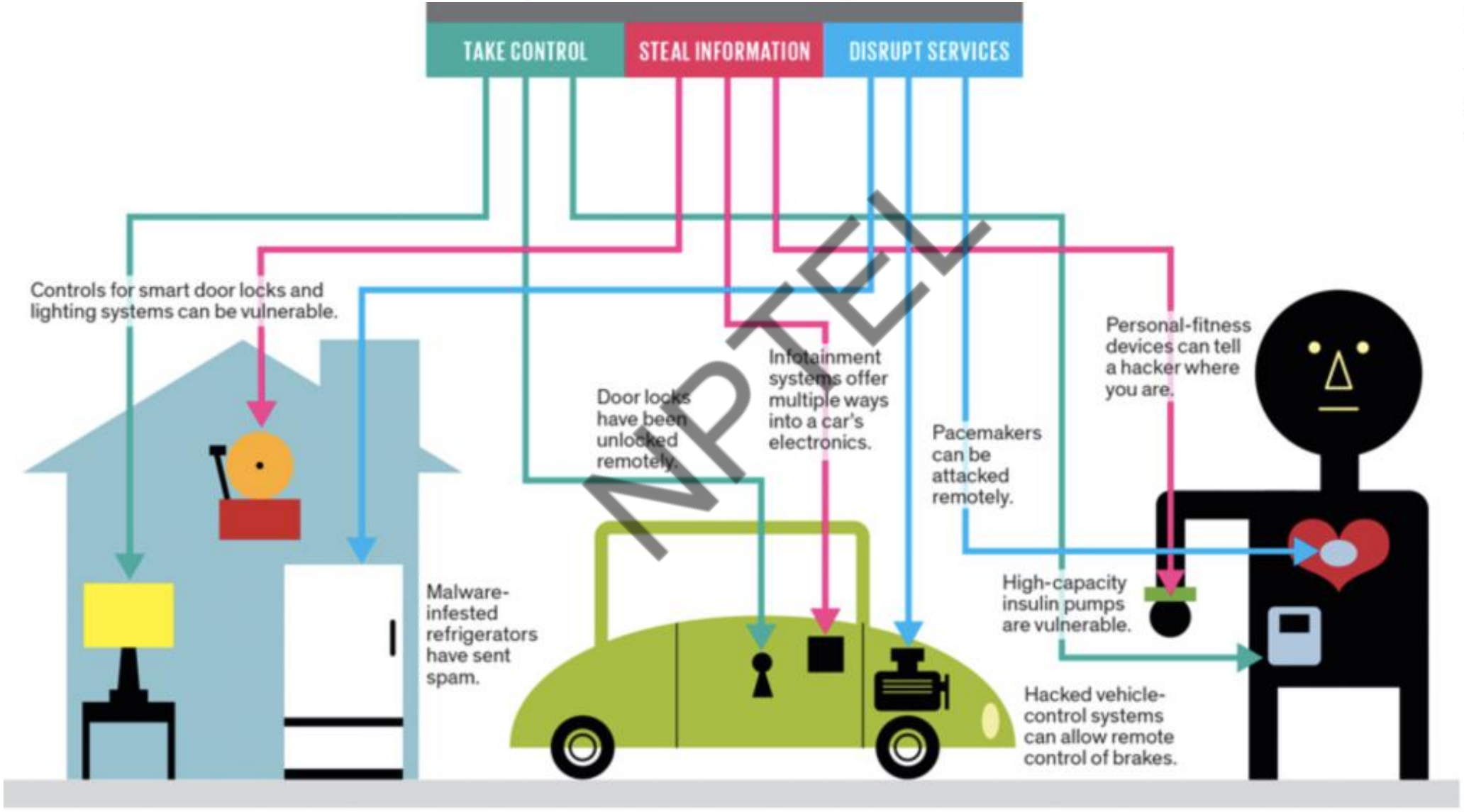



Tradeoff between privacy and QoS

Privacy by Design

- Privacy by design is a process that calls for proactive consideration of privacy objectives and aims from the start, then continues throughout the design and delivery process of products and related actions.
- Seven foundational principles associated with a privacy by design process are:
  - Privacy should be proactive and preventative rather than reactive and remedial
  - Privacy is a default condition rather than an option to be selected
  - Privacy is embedded in the design of a product and is not an add-on
  - Privacy does not impede the full functionality of a product
  - Adequate security measures are applied to protect privacy throughout an entire system wherever sensitive data may travel and throughout the lifecycle of the data.
  - Privacy procedures are visible and transparent to support accountability and trust in delivering on privacy related promises and objectives.
  - Privacy design reflects respect for users' interests and empowers them to manage their data through actions pertaining to consent, accuracy, access, and compliance.

Security Challenges of IoT



Security Challenges of IoT (contd..)

- IoT devices have vulnerabilities due to lack of encryption, insecure web interfaces, inadequate software protection, and insufficient authorization.

- On average, each device contained 25 loopholes, or risks of compromising the home network (HP survey 2014)

- Security challenges may be resolved by training developers to incorporate security solutions (e.g., intrusion prevention systems, firewalls) into products and encouraging users to utilize IoT security features that are built into their devices.

Legal Challenges of IoT

- **Data Ownership and liability issues** : Multiple stakeholders, MGI and M2M communication generated in an IoT environment pose ownership and liability issues.

- **Intellectual Property rights**: When an original data is created by virtue of the interaction of various devices in an IoT environment, which may include, *inter alia*, a new process of arriving at desired results, who claims the IP Rights in such content/data/process?

Chaos challenge of IoT

- In a hyper-connected world, an error in one part of a system can cause disorder throughout.
- A single device may have an insignificant problem, but for the system as a whole, the chain reactions of other connected devices can become disastrous.
- If not designed carefully, multi-purpose devices and collaborative applications can turn our lives into chaos.
- To prevent chaos in the hyper-connected IoT world, businesses need to make effort to reduce the complexity of connected systems, enhance the security and standardization of applications, and guarantee the safety and privacy of users anytime, anywhere.

What is Big Data?

- In order to address the issues of storing and processing huge amounts of data generated by IoT systems Big Data technology comes into picture.
- Huge volume of data produced by both humans and machines, at a very high rate and with massive variety is referred to as Big Data.
- Key enablers for the growth of "Big Data" are:
  - Increase of storage capacities
  - Increase of processing power
  - Increased availability of data

  https://www.youtube.com/watch?v=eVSfJhssXUA

References

- R. De. (2018). MIS Managing Information Systems in Business, Government and Society. Publisher: Wiley. Second Edition.

- I. Lee & K. Lee. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons.* 58, pp. 431-440.

- B. Weinberg, G. Milne, Y. Andonova, & F. Hajjat. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons.* 58, pp.615-624.

Management Information System

Saini Das
Vinod Gupta School of Management, IIT Kharagpur

Module 09: Emerging Technologies

Big Data and other Emerging Technologies

What is Big Data?

- Huge volume of data produced by both humans and machines, at a very high rate and with massive variety is referred to as Big Data.

- Key enablers for the growth of “Big Data” are:
  - Increase of storage capacities
  - Increase of processing power
  - Availability of data

4Vs of Big Data

Volume:

- Around 40,000 exabytes of data are being produced annually.

- Sources of huge volumes of data:
  - Posts, images and videos shared on social media sites
  - Sensors attached to IoT devices
  - Online transactions for banking and e-commerce
  - Scientific research and experiments such as weather analysis
  - Astronomical observations.

4Vs of Big Data (contd..)

Velocity:

- The rate at which data is produced or accumulated is very high.

Source	Volume of Data
YouTube videos	300 hours of video uploaded every minute. This is about 1.6 terabytes of data per minute.
IoT devices	A jet engine produces about 300 gigabytes of data per minute.
Emails	There were 187 million emails generated per minute, worldwide.
Social media	There were more than 455,000 tweets generated per minute. 15 million text messages were sent every minute. Facebook logged 4 million posts per minute (in 2014).

4Vs of Big Data (contd..)

Variety:

- Big Data may be structured, semi-structured or unstructured.
- Unstructured data constitutes almost 80% of Big Data and consists of files that are independent and not relationally linked to other files.
- Examples:
  - Log files from servers
  - Collection of tweets
  - Collection of texts
  - Video or audio posts on social media sites
  - Logs of chat sites

4Vs of Big Data (contd..)

Variety (contd..):

- Semi-structured data has some inherent structure, either corresponding to a hierarchy or graph.
- Lacks relationship between the files
- Often maintained in XML or JSON languages that are readable both by humans and computer programs.
- Data stored in such formats is text-based and one of the major sources of such data is sensors.
- Structured data have some relationships between them

  and is highly organized.

4Vs of Big Data (contd..)

Veracity:

- Refers to the validity of data.
- Data that can used to process for valuable information is called signal; the rest is considered as noise.
- Big data often has noise that is generated at the source.
  - Incorrect names/hashtags; incorrect or misleading addresses
  - Incorrect data readings from sensors; missing data values, etc.
- High values for signal-to-noise ratio are always preferred for Big Data environments.

Technology behind Big Data

- Several Big Data database products are used in the industry such as, Hadoop and Mongo DB.

- These databases are able to process massive volumes of data across distributed databases.

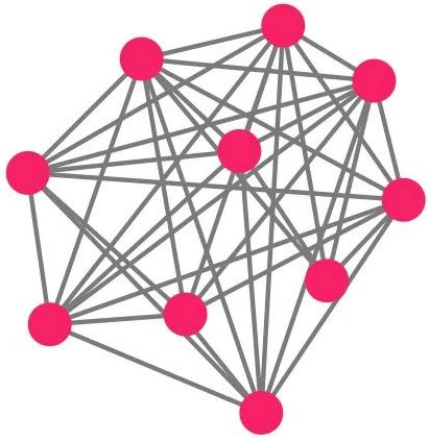
- Their architecture is very different from that of traditional relational databases and is beyond the scope of this course.

Applications of Big Data

- A major U.S airline used publicly available data about weather, flight schedules, and other factors with proprietary data the company itself collected, including feeds from a network of passive radar stations it had installed near airports to gather data about every plane in the local sky, to calculate the ETAs of it's aircrafts at the airports.

- Flipkart collects big data about :
  - customers page visits, logins, product browsing behaviour, bounce off pages, product purchases etc.
  - Logistics
  - Previous 'Big Billion Day' sales.

Blockchain Technology



- Blockchains are software artifacts that enable the creation of public ledgers that are a record of transactions maintained on widely distributed network of clients.
- Once a ledger entry is made it cannot be tampered with and it becomes a permanent entry.
- The entries in the ledger are visible to all collaborating parties.
- The blockchain data is maintained on distributed entries that are secure and cannot be hacked.
- Blockchains provide a proof of authenticity in that only verified and legitimate parties can make the ledger entries.

Applications of Blockchains

- Blockchains are used to manage supply chains. With a blockchain-enabled supply chain, a client can know exactly when a particular shipment has been made by a global supplier, the conditions under which they were stored and transferred and when they will arrive.

- Blockchains can be used by banks who can set up blockchain ledgers for lending money to customers and also recording payments through the system.

- Blockchains can be used for distribution of artistic works, like songs or books directly from songwriters and authors to buyers, without the intermediaries.

Virtual Reality

- **Virtual Reality (VR)** is a computer-generated simulation of an alternate world or reality. It is used in 3D movies and video games. Completely immersive virtual environment. It helps to create simulations similar to the real world and "immerse" the viewer using computers and sensory devices like headsets and gloves. VR is 75% virtual and 25% real.

- Examples:
- Ford Motor Company uses VR to design vehicles.
- At NYU Medical Centre, students wearing 3D-glasses are able to “dissect” a virtual cadaver projected on a screen.

Augmented Reality

- **Augmented Reality (AR)** is a perfect blend of the digital world and the physical elements to create an artificial environment. The system augments the real-world scene. AR is 25% virtual and 75% real.

- Example:
  - Sephora Virtual Artist.
  - Image guided surgery uses AR where images obtained from ultrasound, MRI or CT scans are superimposed on the patient in the operating room.
  - Ikea

References

- K. Laudon and J. Laudon (2016). Management Information Systems Publisher: Pearson. Edition 14e.

- R. De. (2018). MIS Managing Information Systems in Business, Government and Society. Publisher: Wiley. Second Edition.