كلية المنصور الجامعة

Al-Mansour University College

قسم الإعلام الرقمي

المرحلة الرابعه

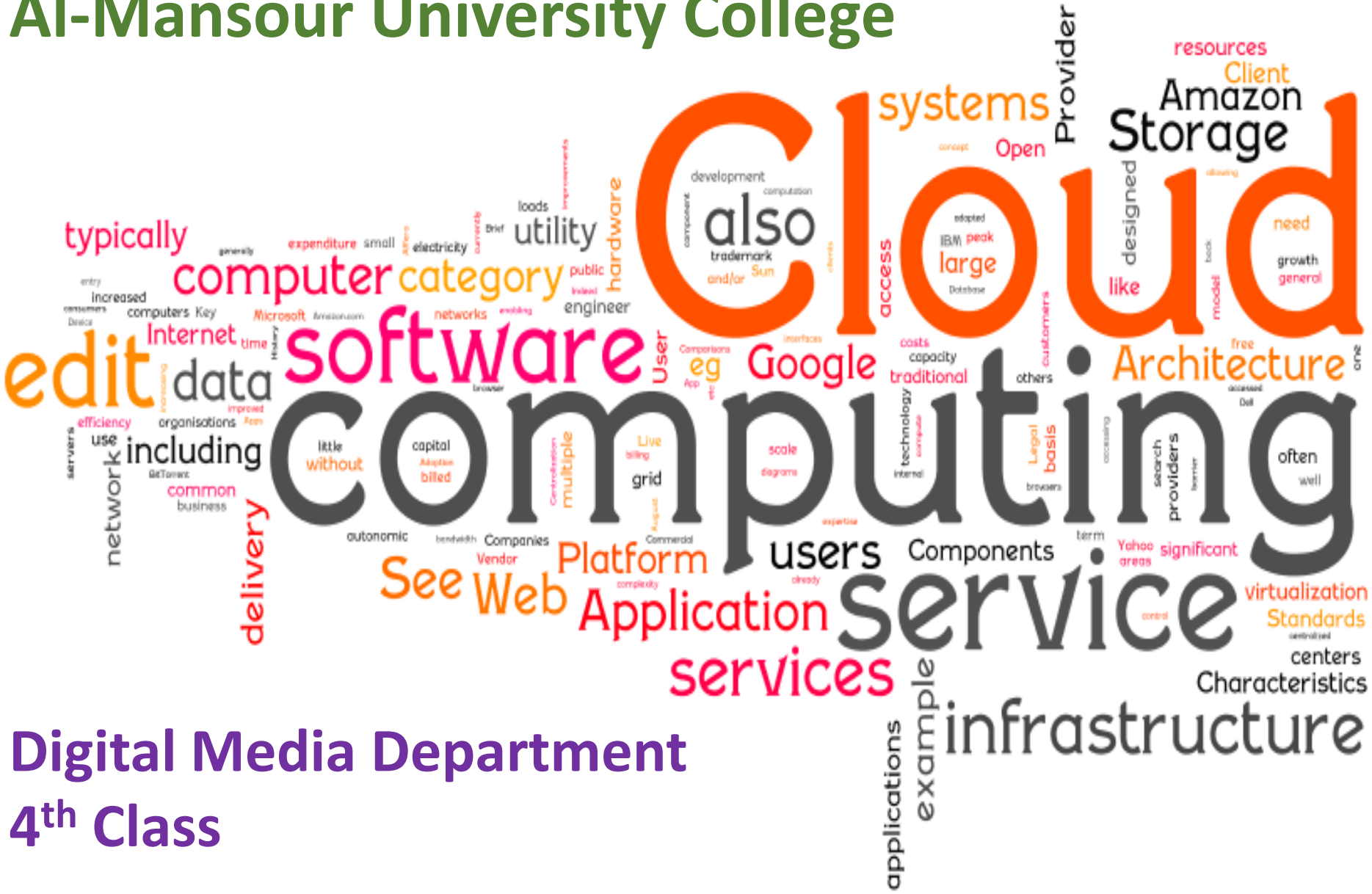
اساسيات الحوسبة السحابية

2023– 2022

2&3

1500

Al-Mansour University College



Digital Media Department

4th Class

Different Cloud Computing Layers

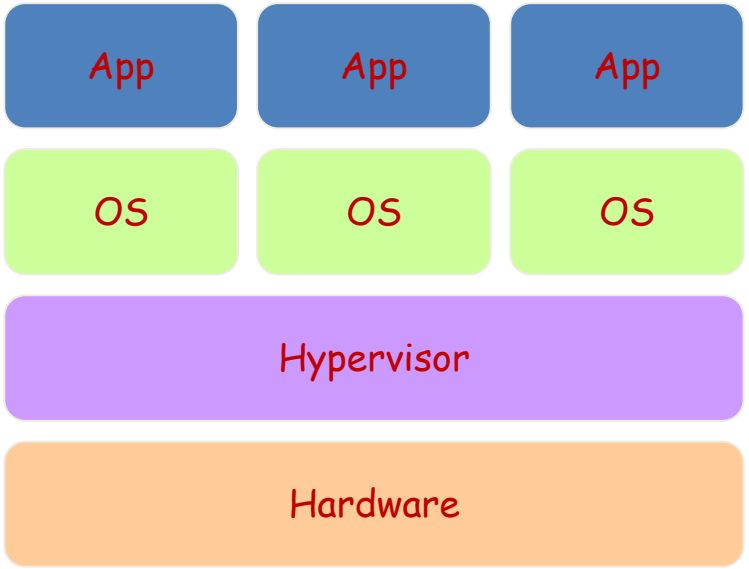
Application Service (SaaS)	MS Live/ExchangeLabs, IBM, Google Apps; Salesforce.com Quicken Online, Zoho, Cisco
Application Platform	Google App Engine, Mosso, Force.com, Engine Yard, Facebook, Heroku, AWS
Server Platform	3Tera, EC2, SliceHost, GoGrid, RightScale, Linode
Storage Platform	Amazon S3, Dell, Apple, …

Cloud Computing Service Layers

	Services	Description
Application Focused	Services	Services – Complete business services such as PayPal, OpenID, OAuth, Google Maps, Alexa
	Application	Application – Cloud based software that eliminates the need for local installation such as Google Apps, Microsoft Online
	Development	Development – Software development platforms used to build custom cloud based applications (PAAS & SAAS) such as SalesForce
Infrastructure Focused	Platform	Platform – Cloud based platforms, typically provided using virtualization, such as Amazon ECC, Sun Grid
	Storage	Storage – Data storage or cloud based NAS such as CTERA, iDisk, CloudNAS
	Hosting	Hosting – Physical data centers such as those run by IBM, HP, NaviSite, etc.

Virtualization

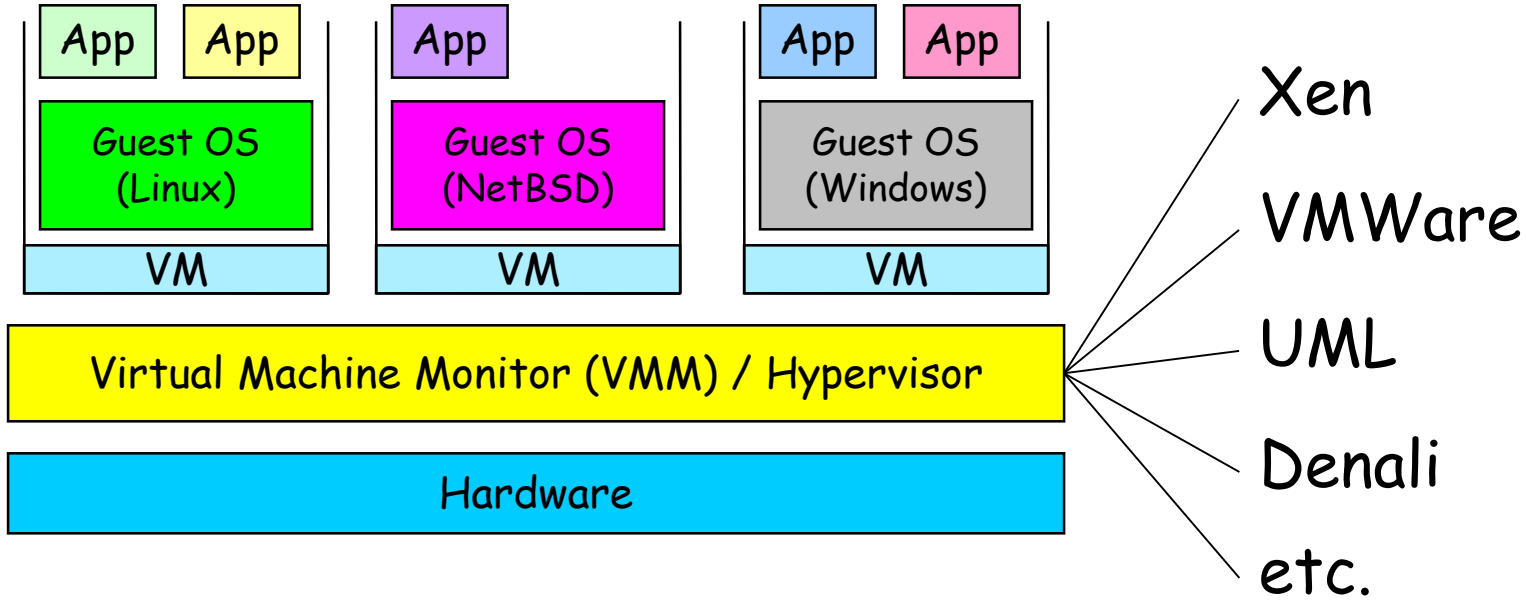
- Virtual workspaces:
  - An abstraction of an execution environment that can be made dynamically available to authorized clients by using well-defined protocols,
  - Resource quota (e.g. CPU, memory share),
  - Software configuration (e.g. O/S, provided services).
- Implement on Virtual Machines (VMs):
  - Abstraction of a physical host machine,
  - Hypervisor intercepts and emulates instructions from VMs, and allows management of VMs,
  - VMWare, Xen, etc.
- Provide infrastructure API:
  - Plug-ins to hardware/support structures



Virtualized Stack

Virtual Machines

- VM technology allows multiple virtual machines to run on a single physical machine.



Performance: Para-virtualization (e.g. Xen) is very close to raw physical performance!

What is the purpose and benefits?

- Cloud computing enables companies and applications, which are system infrastructure dependent, to be infrastructure-less.
- By using the Cloud infrastructure on “pay as used and on demand”, all of us can save in capital and operational investment!
- Clients can:
  - Put their data on the platform instead of on their own desktop PCs and/or on their own servers.
  - They can put their applications on the cloud and use the servers within the cloud to do processing and data manipulations etc.

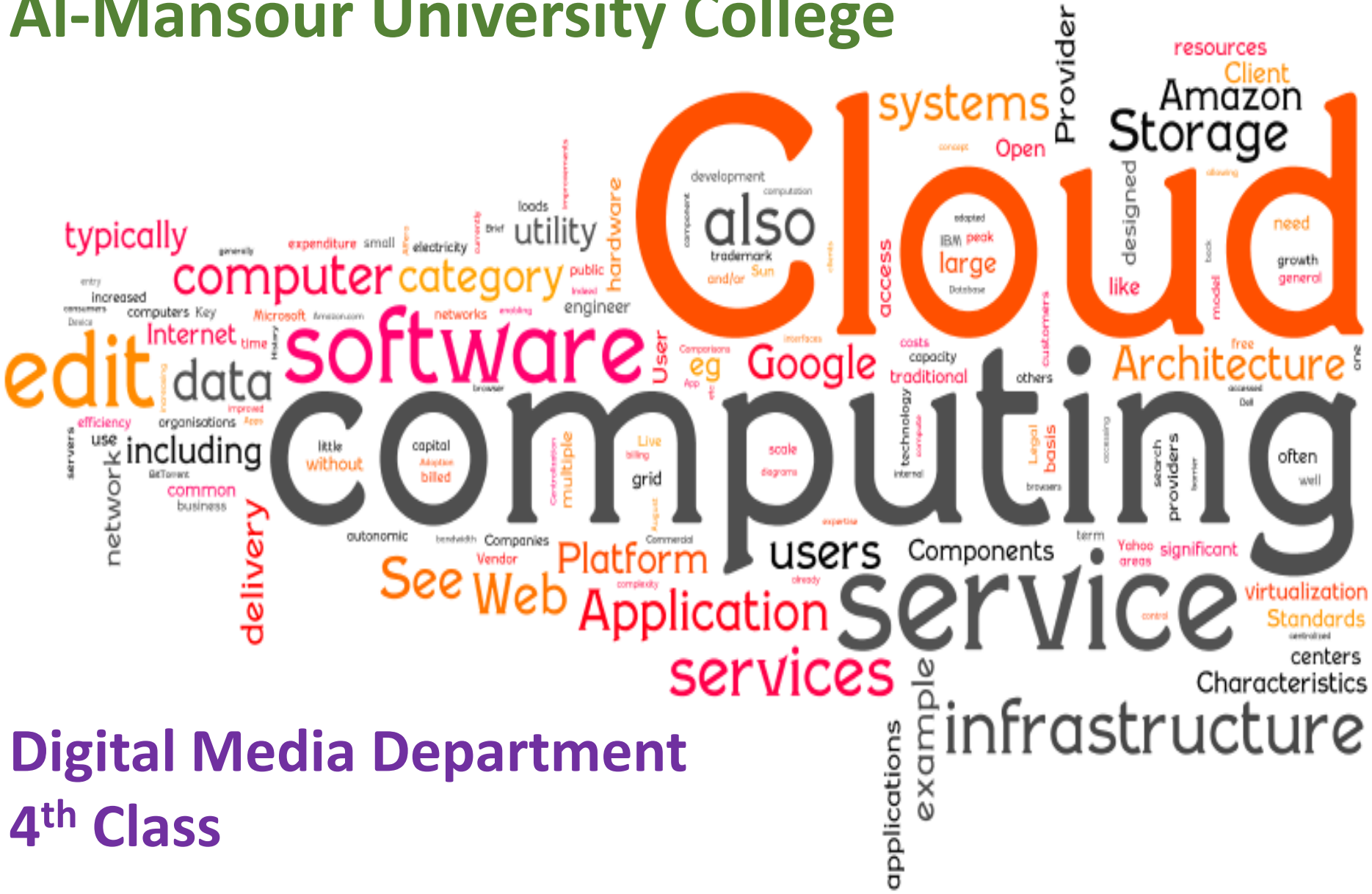
7

Cloud-Sourcing

- Why is it becoming a Big Deal:
  - Using high-scale/low-cost providers,
  - Any time/place access via web browser,
  - Rapid scalability; incremental cost and load sharing,
  - Can forget need to focus on local IT.
- Concerns:
  - Performance, reliability, and SLAs,
  - Control of data, and service parameters,
  - Application features and choices,
  - Interaction between Cloud providers,
  - No standard API – mix of SOAP and REST!
  - Privacy, security, compliance, trust…

8

Al-Mansour University College



Security and Privacy Issues in Cloud Computing

- Infrastructure Security
  - Network Level
  - Host Level
  - Application Level
- Data Security and Storage
- Privacy

- And more…

The Network Level

- Ensuring confidentiality and integrity of your organization's data-in-transit to and from your public cloud provider
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider
- Ensuring availability of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers
- Replacing the established model of network zones and tiers with domains

The Host Level

- SaaS/PaaS
  - Both the PaaS and SaaS platforms abstract and hide the host OS from end users
  - Host security responsibilities are transferred to the CSP (Cloud Service Provider)
- IaaS Host Security
  - Virtualization Software Security
    - Hypervisor (also called Virtual Machine Manager (VMM)) security is a key
      - a small application that runs on top of the physical machine H/W layer
      - implements and manages the virtual CPU, virtual memory, event channels, and memory shared by the resident VMs
      - Also controls I/O and memory access to devices.
    - Bigger problem in multitenant architectures
  - Customer guest OS or Virtual Server Security
    - The virtual instance of an OS
    - Vulnerabilities have appeared in virtual instance of an OS
    - e.g., VMWare, Xen, and Microsoft's Virtual PC and Virtual Server
    - Customers have full access to virtual servers.

Local Host Security

- Are local host machines part of the cloud infrastructure?
  - Outside the security perimeter
  - While cloud consumers worry about the security on the cloud provider's site, they may easily forget to harden their own machines
- The lack of security of local devices can
  - Provide a way for malicious services on the cloud to attack local networks through these terminal devices
  - Compromise the cloud and its resources for other users

Local Host Security (Cont.)

- With mobile devices, the threat may be even stronger
  - Users misplace or have the device stolen from them
  - Security mechanisms on handheld gadgets are often times insufficient compared to say, a desktop computer
  - Provides a potential attacker an easy avenue into a cloud system.
  - If a user relies mainly on a mobile device to access cloud data, the threat to availability is also increased as mobile devices malfunction or are lost
- Devices that access the cloud should have
  - Strong authentication mechanisms
  - Tamper-resistant mechanisms
  - Strong isolation between applications
  - Methods to trust the OS
  - Cryptographic functionality when traffic confidentiality is required

The Application Level

- DoS
- EDoS(Economic Denial of Sustainability)
  - An attack against the billing model that underlies the cost of providing a service with the goal of bankrupting the service itself.
- End user security
- Who is responsible for Web application security in the cloud?
- SaaS/PaaS/IaaS application security
- Customer-deployed application security

Data Security and Storage

- Several aspects of data security, including:
  - Data-in-transit
    - Confidentiality + integrity using secured protocol
    - Confidentiality with non-secured protocol and encryption
  - Data-at-rest
    - Generally, not encrypted , since data is commingled with other users' data
    - Encryption if it is not associated with applications?
      - But how about indexing and searching?
      - Then homomorphic encryption vs. predicate encryption?
  - Processing of data, including multitenancy
    - For any application to process data, not encrypted

Data Security and Storage

- Data remanence
- Inadvertent disclosure of sensitive information is possible
- Data security mitigation?
- Do not place any sensitive data in a public cloud
- Encrypted data is placed into the cloud?
- Provider data and its security: storage
- To the extent that quantities of data from many companies are centralized, this collection can become an attractive target for criminals
- Moreover, the physical security of the data centre and the trustworthiness of system administrators take on new importance.

What is Privacy?

- The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions.
- It is shaped by public expectations and legal interpretations; as such, a concise definition is elusive if not impossible.
- Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data (or Personally Identifiable Information—PII).
- At the end of the day, privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization's practice around personal information.

What Are the Key Privacy Concerns?

- Typically mix security and privacy
- Some considerations to be aware of:
  - Storage
  - Retention
  - Destruction
  - Auditing, monitoring and risk management
  - Privacy breaches
  - Who is responsible for protecting privacy?

From [6] Cloud Security and Privacy by Mather and Kumaraswamy