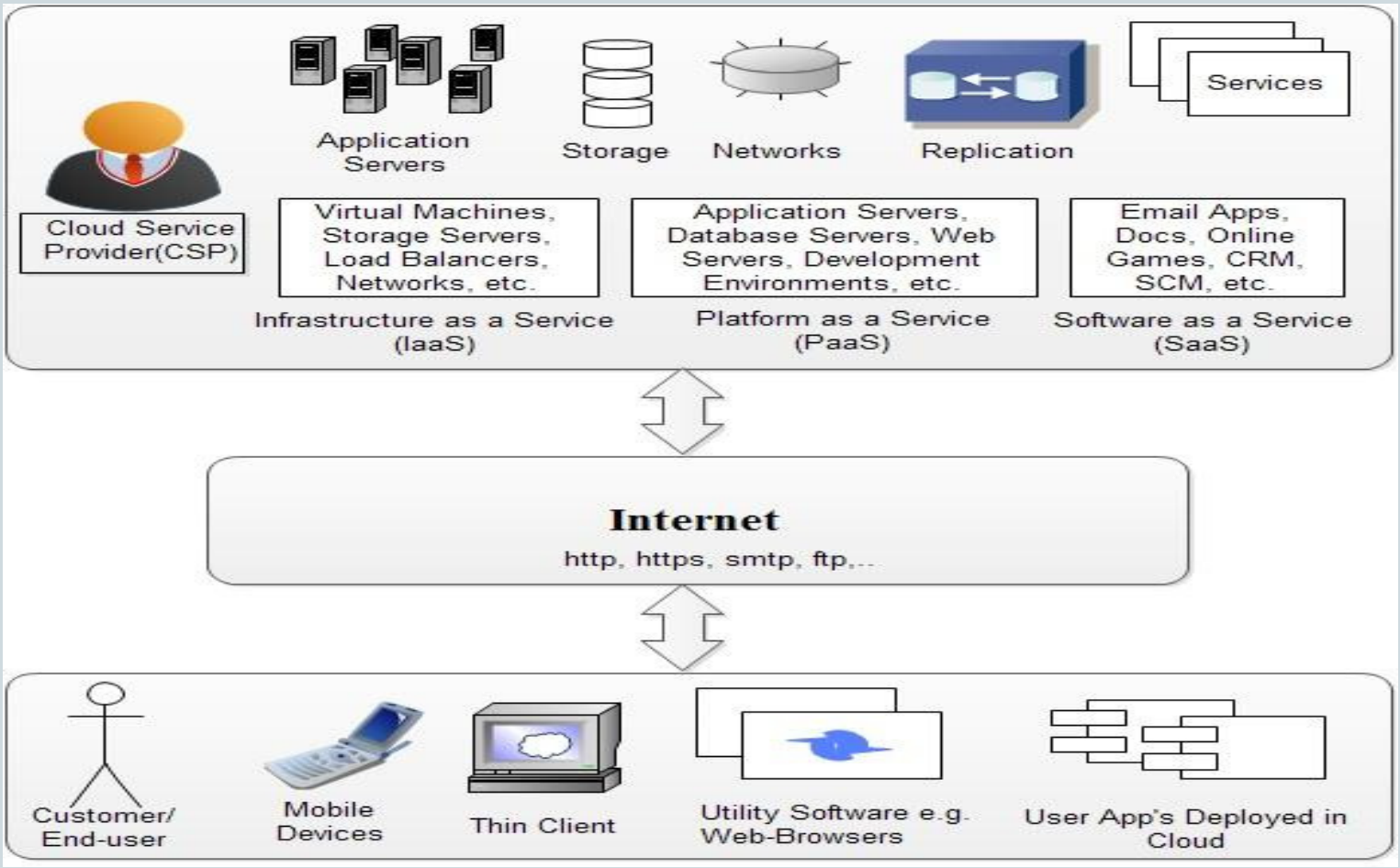
Cloud Computing Security Analysis

PRESENTED BY: AHMED OSMAN
CS591

Agenda

- What is Cloud?
- What are the Pros & Cons?
- Security Analysis
- Summary

What is Cloud



Pros. & Cons.

- **Pros.**
  - Reduced costs
  - Resource sharing is more efficient
  - Management moves to cloud provider
  - Dynamic resource availability for crunch periods
  - Consumption based cost
  - Resource sharing is more efficient
  - Faster time to roll out new services

- **Cons.**
  - Compliance/regulatory laws mandate on-site ownership of data
  - Security and privacy Latency & bandwidth guarantees
  - Availability & reliability
  - Uncertainty around interoperability, portability & lock in
  - Absence of robust SLAs

Security Analysis

- **Identify Assets**
  - Customer Data
  - Customer Applications
  - Client Computing Devices

- **Identify Threats**
  - Failures in Provider Security
  - Attacks by Other Customers
  - Availability and Reliability Issues
  - Legal and Regulatory Issues
  - Perimeter Security Model Broken
  - Integrating Provider and Customer Security Systems

Failures in Provider Security

- **Explanation**
  - Provider controls servers, network, etc.
  - Customer must trust provider's security
  - Failures may violate CIA principles

- **Countermeasures**
  - Verify and monitor provider's security

Attacks by Other Customers

- **Threats**
  - Provider resources shared with untrusted parties like CPU, storage, network
  - Customer data and applications must be separated
  - Failures will violate CIA principles
- **Countermeasures**
  - Hypervisors for compute separation
  - MPLS, VPNs, VLANs, firewalls for network separation
  - Cryptography (strong)
  - Application-layer separation (less strong)

Availability and Reliability Issues

- **Threats**
  - Clouds may be less available than in-house IT
    - Complexity increases chance of failure
    - Clouds are prominent attack targets
    - Internet reliability is spotty
    - Shared resources may provide attack vectors
  - BUT cloud providers focus on availability
- **Countermeasures**
  - Evaluate provider measures to ensure availability
  - Monitor availability carefully
  - Plan for downtime
  - Use public clouds for less essential applications

Summary

- Engage in full risk management process for each case
- For small and medium organizations
  - Cloud security may be a big improvement!
  - Cost savings may be large (economies of scale)
- For large organizations
  - Already have large, secure data centers
  - Main sweet spots:
    - Elastic services
    - Internet-facing services
- Employ countermeasures listed above

Questions ?