

CS 4037

Introduction to Cloud

Computing

Lecture 3

Danyal Farhat

FAST School of Computing

NUCES Lahore

Understanding Cloud Computing – Part 2

Lecture's Agenda

- Origins and Influences
- Basic Concepts and Terminologies
- **Goals and Benefits**
- Risks and Challenges



Reduced Investment and Proportional Costs

- Cloud environments are comprised of highly extensive infrastructure that offers pools of IT resources that can be leased using a pay-for-use model whereby only the **actual usage of the IT resources is billable**.
- When compared to equivalent on-premise environments, clouds provide the potential for **reduced initial investments** and operational costs proportional to measured usage.

Increased Scalability

- The inherent ability of a cloud to scale IT resources enables organizations to accommodate unpredictable usage fluctuations without being limited by pre-defined thresholds that may turn away usage requests from customers.
- The ability of a cloud to decrease required scaling is a feature that relates directly to the proportional costs benefit.

Increased Availability and Reliability

- By leveraging cloud to make IT resources highly available and reliable, organizations are able to **increase quality-of service guarantees** to customers and reduce or **avoid potential loss of business** resulting from unanticipated runtime failures.
- Although many cloud platforms are capable of offering remarkably high levels of availability and reliability, it **comes down to the guarantees made in the SLA** that represent their actual contractual obligations.

Lecture's Agenda

- Origins and Influences
- Basic Concepts and Terminologies
- Goals and Benefits
- **Risks and Challenges**



Increased Security Vulnerabilities

- The moving of business data to the cloud means that the **responsibility over data security** becomes shared with the cloud provider.
- The extent to which the data is secure is now **limited** to the security controls and policies applied by both the cloud consumer and cloud provider.
- The **overlapping of organizations' trust boundaries** provide malicious cloud consumers with greater opportunities to attack IT resources and steal or damage business data.
- It can be **challenging** for the cloud provider to offer security mechanisms that accommodate the security requirements of multiple cloud service consumers.

Increased Security Vulnerabilities (Cont.)

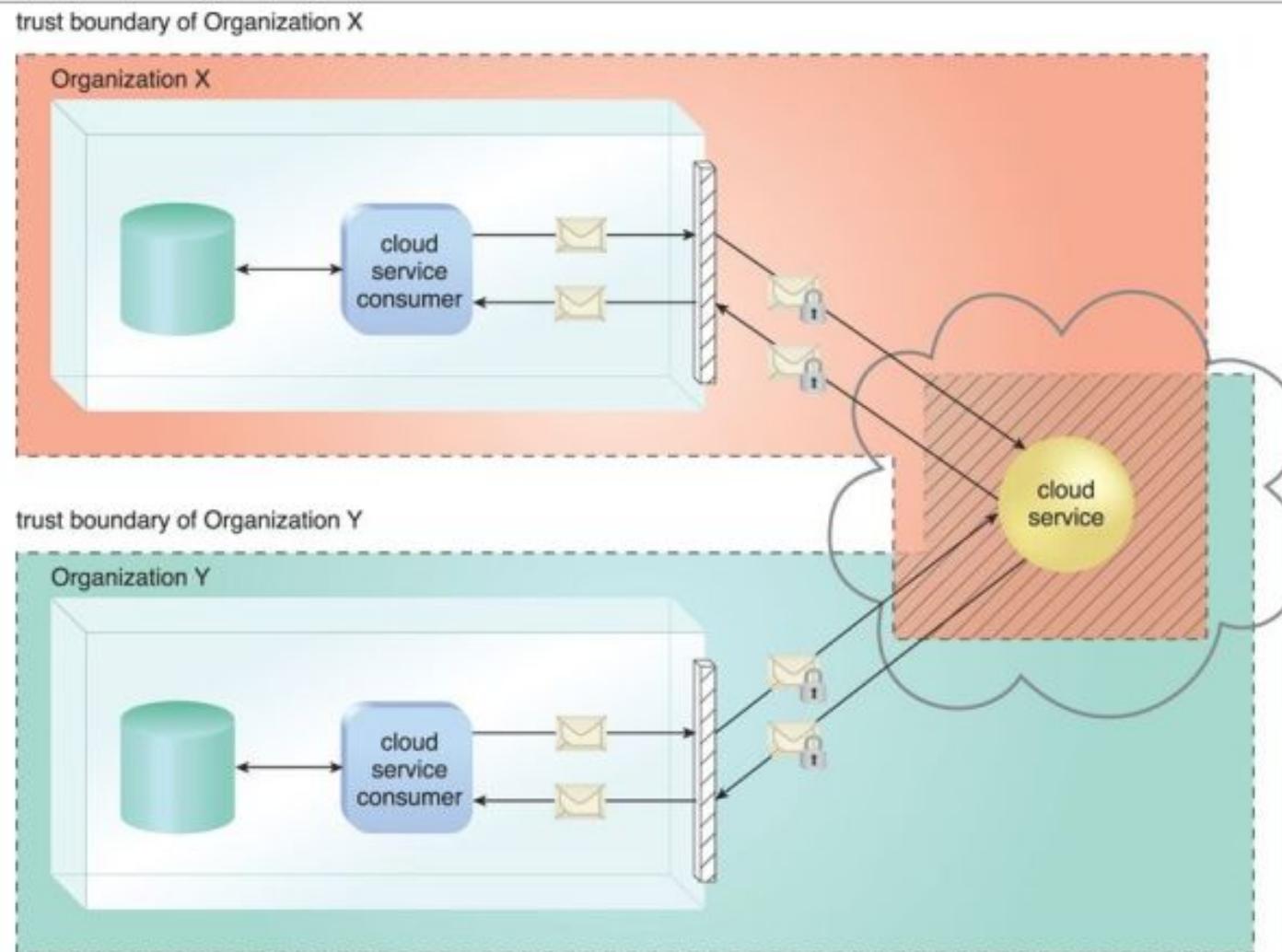
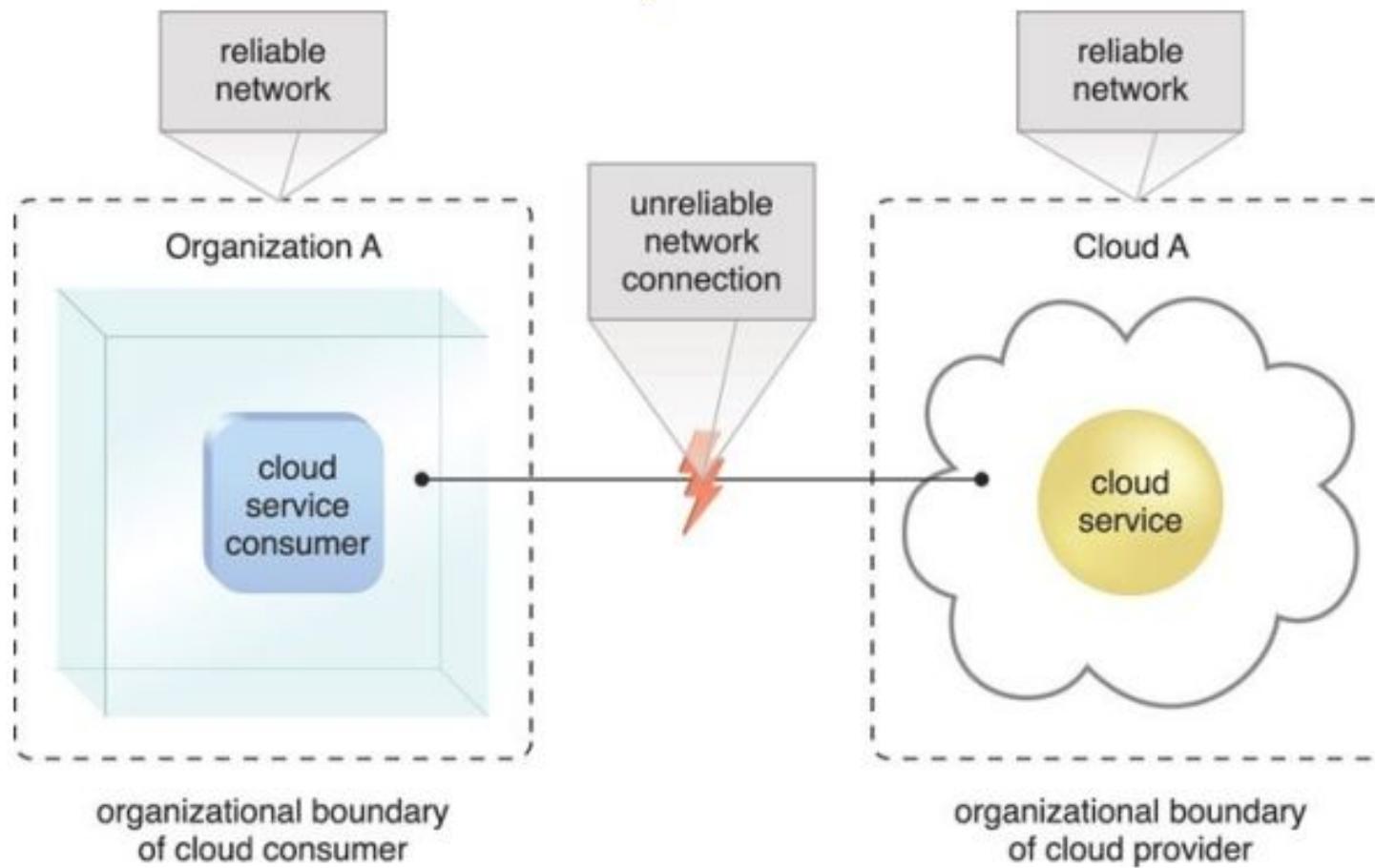


Figure 3.9. The shaded area with diagonal lines indicates the overlap of two organizations' trust boundaries.

Reduced Operational Governance Control

- A cloud consumer's **operational governance is limited** within cloud environments due to the control exercised by a cloud provider over its platforms.
- An unreliable cloud provider **may not maintain the guarantees** it makes in the SLAs that were published for its cloud services. This can jeopardize the quality of the cloud consumer solutions that rely on these cloud services.
- Longer geographic distances between the cloud consumer and cloud provider can require additional network hops that introduce **fluctuating latency** and potential bandwidth constraints.

Reduced Operational Governance Control (Cont.)



Limited Portability Between Cloud Providers

- Portability is a **measure used to determine** the impact of moving cloud consumer IT resources and data between clouds.
- Due to a lack of established industry standards within the cloud computing industry, public clouds are commonly **proprietary** to various extents.
- For cloud consumers that have custom-built solutions with dependencies on proprietary cloud environments, it can be challenging to move from one cloud provider to another.

Limited Portability Between Cloud Providers (Cont.)

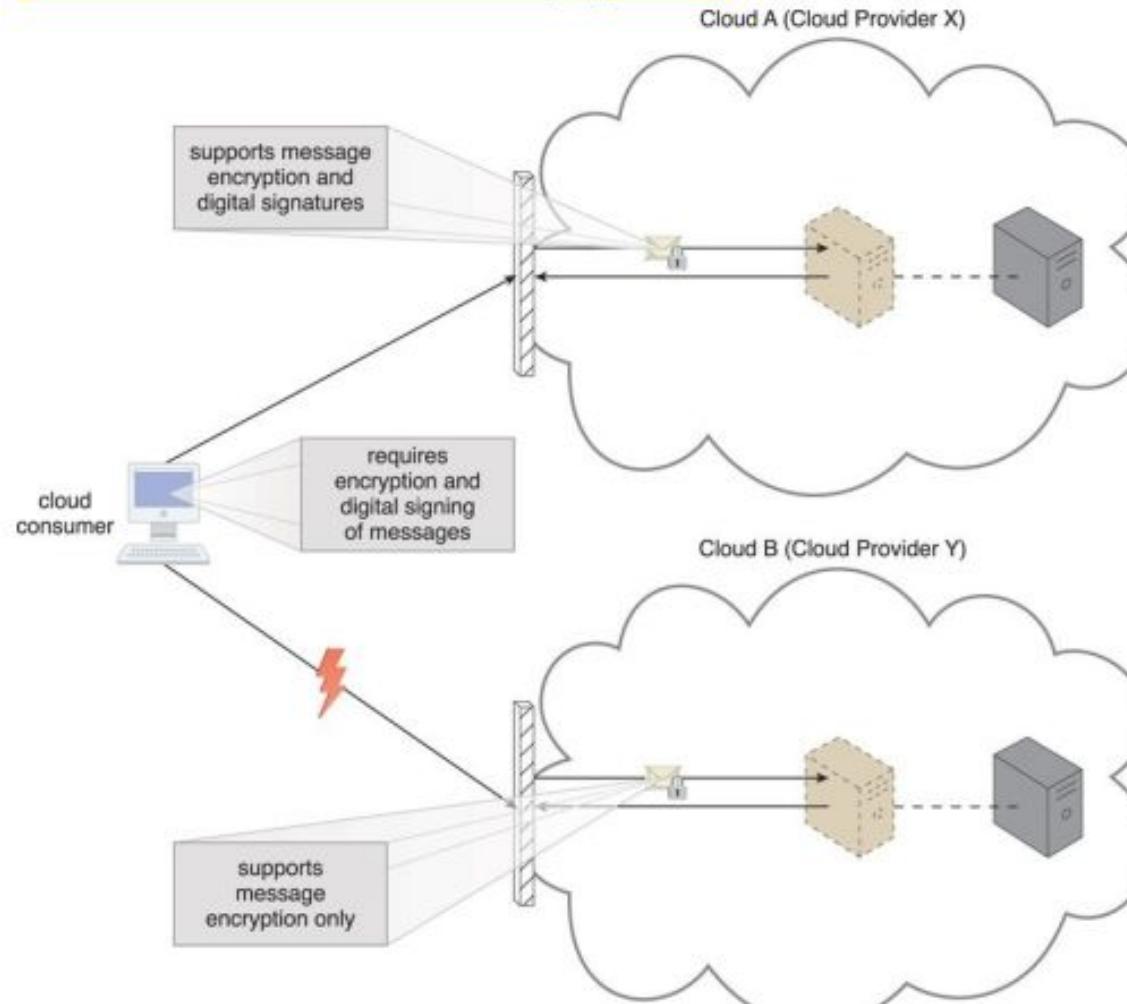


Figure 3.11. A cloud consumer's application has a decreased level of portability when assessing a potential migration from Cloud A to Cloud B, because the cloud provider of Cloud B does not support the same security technologies as Cloud A.

Multi-Regional Compliance and Legal Issues

- The geographical location of data and IT resources can be out of a cloud consumer's control when hosted by a third-party cloud provider. This can introduce various legal and regulatory compliance concerns.

Examples:

- Some UK laws require personal data belonging to UK citizens to be kept within the United Kingdom.
- An European cloud consumer's data that is located in the U.S. is easily accessible by the US government agencies (due to the U.S. Patriot Act) when compared to data located in many European Union countries.

Additional Resources

- Cloud Computing – Concepts, Technology, and Architecture by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

□ Chapter 3: Understanding Cloud Computing

Questions?