

Overview of Cloud Computing Security

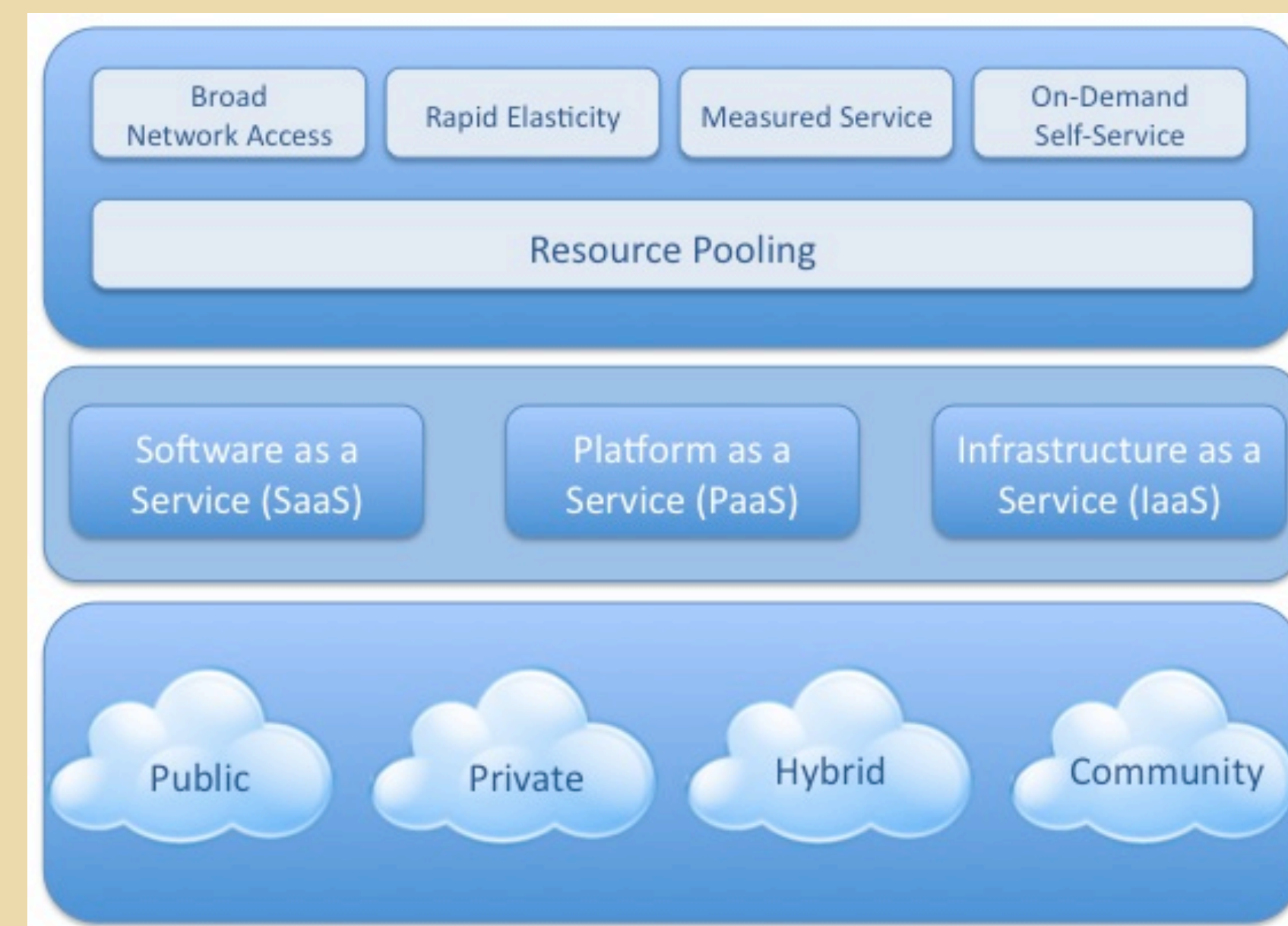
Madhuri Revalla, Ajay K. Gupta, College of Engineering and Applied Sciences
Western Michigan University, Kalamazoo, MI - 49008



WESTERN MICHIGAN UNIVERSITY

1. Overview

Cloud computing is the most significant shift in Information Technology.



Characteristics

Service Models

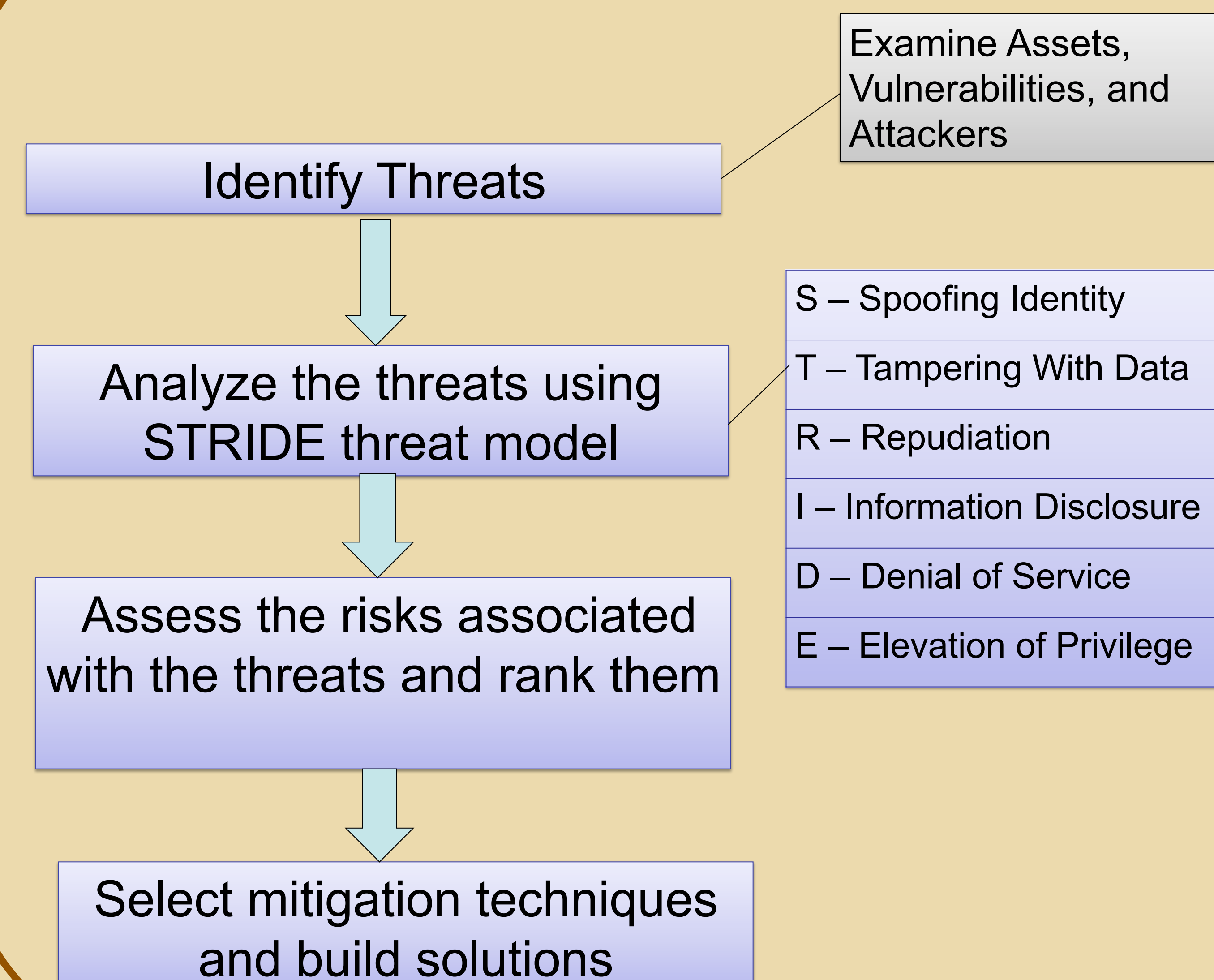
Deployment Models

Visual Model of Cloud Computing [NIST]

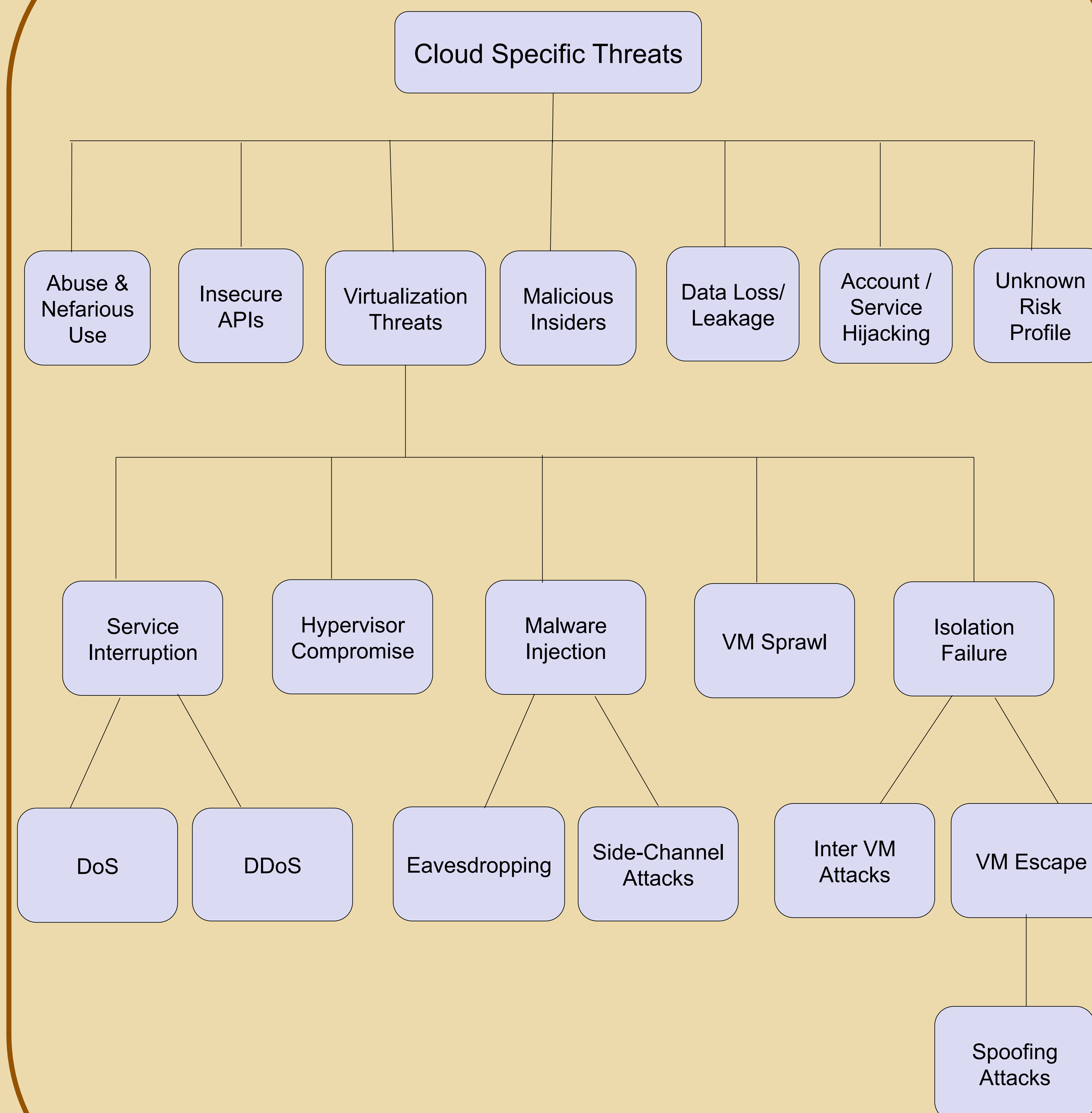
2. Motivation

- Cloud provider - provides resources/services that can be accessed from anywhere in the world by the user.
- Cloud user - can be either a single person or any organization.
- Cloud computing has many benefits, but security is a big concern.
- Cloud provider should provide privacy and security to the user's data and applications.

3. Threat Model



4. Threats in Cloud Computing



6. Data privacy

The two issues lead to many privacy and security concerns:

1. User does not have control over the data
2. Dependence on the cloud provider

Solution: Data encryption, but should consider the facts

- How to encrypt the data
- Who is responsible for encryption

- ◆ Choose a strong encryption mechanism to secure data in cloud computing.
- ◆ To ensure privacy, data should be encrypted by the user.

Next Question: How to authenticate the user?

- ✓ Use Public Key Infrastructure (PKI)
PKI provides Authentication, Integrity, Confidentiality.

7. Authentication

PKI is the strong authentication system, but does not replace the need for authentication.

Use two-factor authentication – In combination with the other factors such as Smart cards or Biometrics, PKI can create solution for authentication

8. Conclusions

Traditional security techniques are not capable enough to handle cloud specific threats.

To secure cloud, cloud specific security mechanisms need to be investigated and developed.

5. Shared Technology Vulnerabilities

Cloud computing provides scalable services with shared infrastructure, computational power, storage, and cost-effectiveness over the Internet on user's demand basis.

- Virtualization plays a major role in cloud computing
 - Normal virtualization security techniques are not enough to handle virtualization security in cloud computing
 - Applying virtualization to cloud computing may cause additional security risks such as isolation failure, service interruption
- Multiple users share the cloud infrastructure
 - This co-tenancy also introduce vulnerabilities such as performing side-channel attacks to get another user's confidential information via information leakage