ADC501

Cloud Computing

Module 5

Security

Data Security

complex data security challenges in cloud

- confidential business, government, or regulatory data
- multiple tenants sharing the same infrastructure
- legal issues - Data Privacy Directive
- CSPs securely recycle disk space and erase existing data
- Loss of visibility to key security and operational intelligence
- A new type of insider

The issues that must be addressed are as follows:

Breach notification and data residency - businesses should categorize data

Data management at rest - Storage used for archive and backup is encrypted , a strong identity and access management policy

Data protection in motion - secure communication protocols such as Secure Socket Layer (SSL)/Transport Layer Security (TLS) for browser access or virtual private network (VPN)

Data Center Security

- virtual infrastructure, or the virtual machine (VM)
- network and storage – of data center
- *Lack of performance and availability* - cryptographic processing applications for SSL, do not fare well when virtualized , Even smaller issues such as IP address availability can be impacted by virtualization sprawl
- *Lack of application awareness* – applications might encounter performance issues
- *Additional, unanticipated costs* - VMs begin to burden the existing infrastructure
- *Unused virtualization features* –
- *Overflowing storage network* - file storage becomes unmanageable
- *Congested storage network*
- *Management complexity* - The hypervisor and the host system, Managing VMs, application network, and storage network together

- Access Control
- Encryption and Decryption
- Logging of all user and administrator access to cloud resources
- images captured by migration or snapshotting tools

Virtualization Security

Virtualization mainly focuses on three different areas

virtual networks (network virtualization), storage virtualization, and server virtualization

- *A new threat* - If the hypervisor is vulnerable to exploit
- *Storage concerns* – local storage associated with VMs, clear data upon resource release/allocation
- *Traffic management*

Network Security

- *Application performance* - Cloud tenants should be able to specify bandwidth requirements for applications hosted in the cloud , to satisfy user transactions within an acceptable time frame and meet predefined service-level agreements (SLAs)

- *Flexible deployment of appliances* - deep packet inspection (DPI) or intrusion detection systems (IDSs),

- *Policy enforcement complexities* - Traffic isolation and access control to end users

- *Topology-dependent complexity*

- *Application rewriting*

- *Location dependency*

- *Multilayer network complexity* - three-layer data center network includes a TOR (Top of Rack) layer connecting the servers in a rack, an aggregation layer, and a core layer

Security Issues in Cloud Service Models

Software-as-a-Service Security Issues

points of concern in SaaS are as follows

- *Network security* - SSL and TLS for security
- *Resource locality*
- *Cloud standards*
- *Data segregation -* segregate the data from different users
- *Data access*
- *Data breaches*
- *Backup*
- *Identity management (IdM) and sign-on process*

Platform-as-a-Service Security Issues

- secure communications and access control

Infrastructure-as-a-Service Security Issues

- *Hypervisor security*
- *Multitenancy*
- *Identity management and access control (IdAM)*
- *Network security*

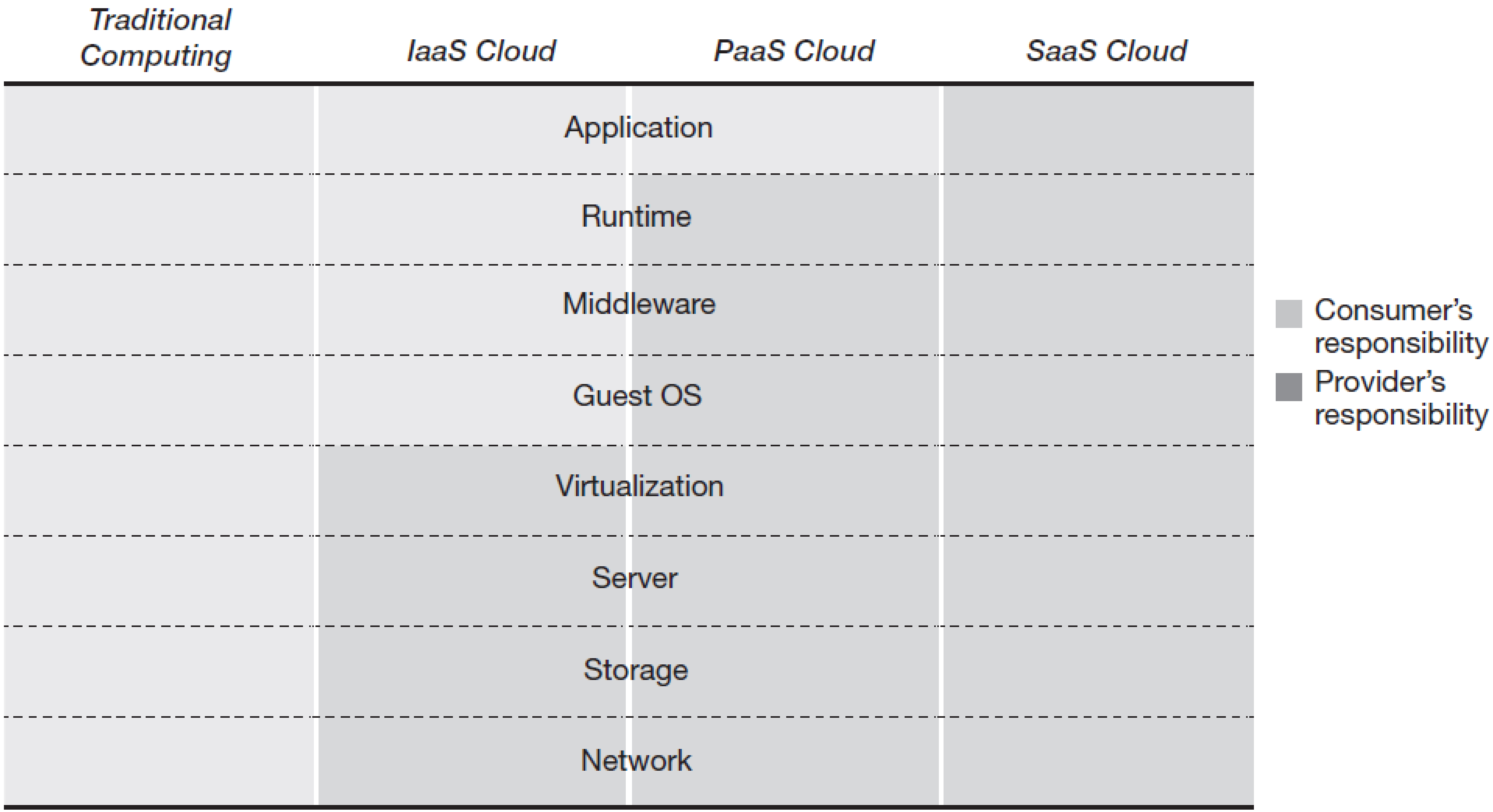

FIG 6.5: Share of security management responsibilities in traditional computing and cloud service environment

Elements of Cloud Security Model

Cloud consumers must query to the service providers regarding these issues

- *Privileged user access* - user means ‘users’ at the provider’s end who are managing the cloud
- *Regulatory compliance -* consumers should opt for providers who have obtained security certifications
- *Data location*
- *Data segregation*
- *Recovery*
- *Investigative support -* Investigation of inappropriate or illegal activity
- *Long-term viability*

Cloud Security Alliance (CSA)

focused on the promotion of a secured cloud computing environment

organization is registered as a non-profit corporation in Washington in United States

recommends the best practices and offers guidance for security maintenance in cloud

offered a certification program for service providers known as ‘CSA Security, Trust and Assurance Registry’ (STAR) for self-assessment of providers

The Cloud Cube Model

- Cloud security reference model
- Jericho Forum proposed Cloud Cube Model in 2009
- defining a three-dimensional cube
- presents four criteria to differentiate various types of cloud formations
- *The Four Criteria*

  1. Whether data will be stored internally within *physical boundary* of the organization or to some external location?

  2. Will the cloud be formed using *proprietary technology* (technology that is property of someone) of some computing firm or by using *open technology* that is open to everyone for use? It is to note that, here 'technology' means 'cloud technology' or operating standard of cloud.

  3. Whether the cloud will operate within organization's *network boundary* (the logical security perimeter) only or outside the boundary also?

  4. Will the development and maintenance of the cloud service be outsourced to some third party or will be done with in-house team?

- These dimensions are –

- **Data Boundary: Internal (I) / External (E)**

- **Ownership: Proprietary (P) / Open (O)**

- **Security Boundary: Perimeterized (Per) / De-perimeterized (D-p)**

- **Sourcing: Insourced / Outsourced**

IP, IO, EP and EO
Per (IP, IO, EP, EO) and D-p (IP, IO, EP, EO)
Sourcing can either be outsourced or insourced for each of the eight cloud forms

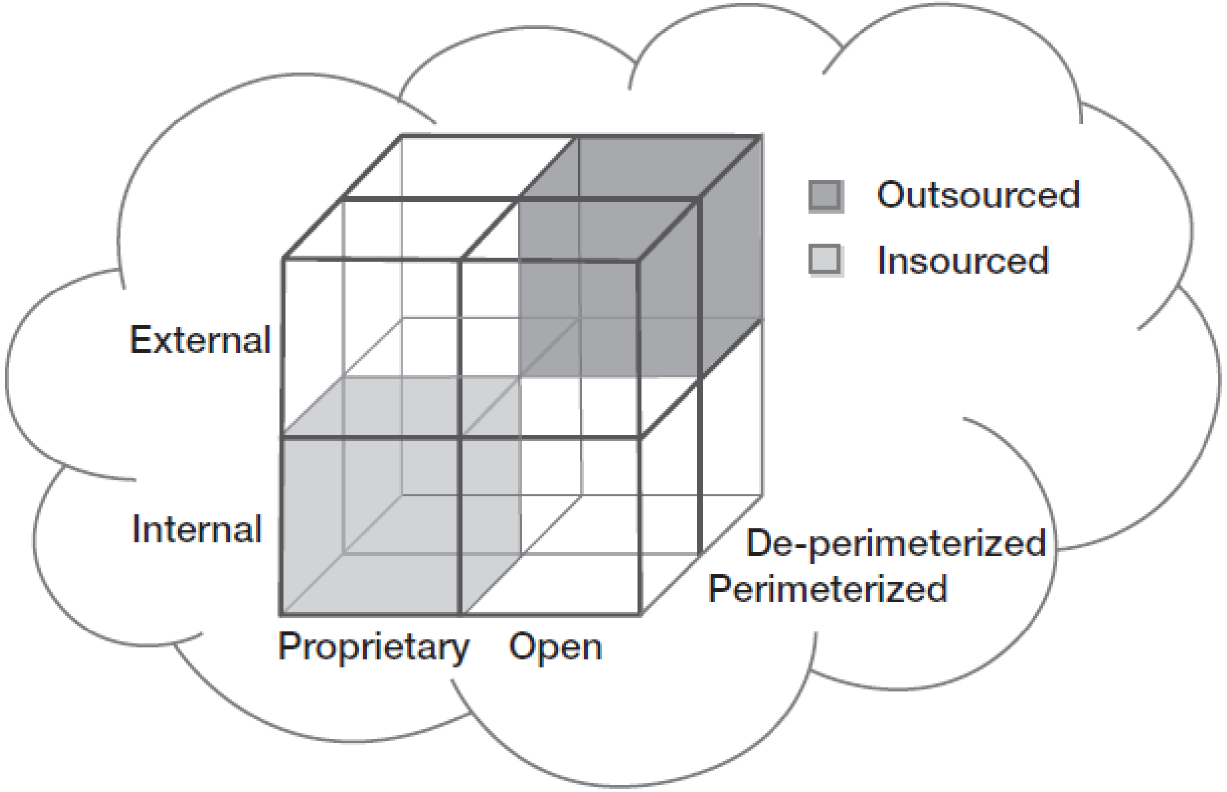

FIG 6.4: Jericho Forum's Cloud Cube Model[7]

- top-right-rear E / O / D-p cloud formation is considered as the one where optimal flexibility and collaboration can be achieved

- bottom-left-front I / P / Per cloud formation is the most restricted one