Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 13

Cloud and IoT Security

Cloud Computing:

- NIST defines cloud computing, in NIST SP-800-145 (*The NIST Definition of Cloud Computing*, September 2011*)* as follows:

  "**Cloud computing:** A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."

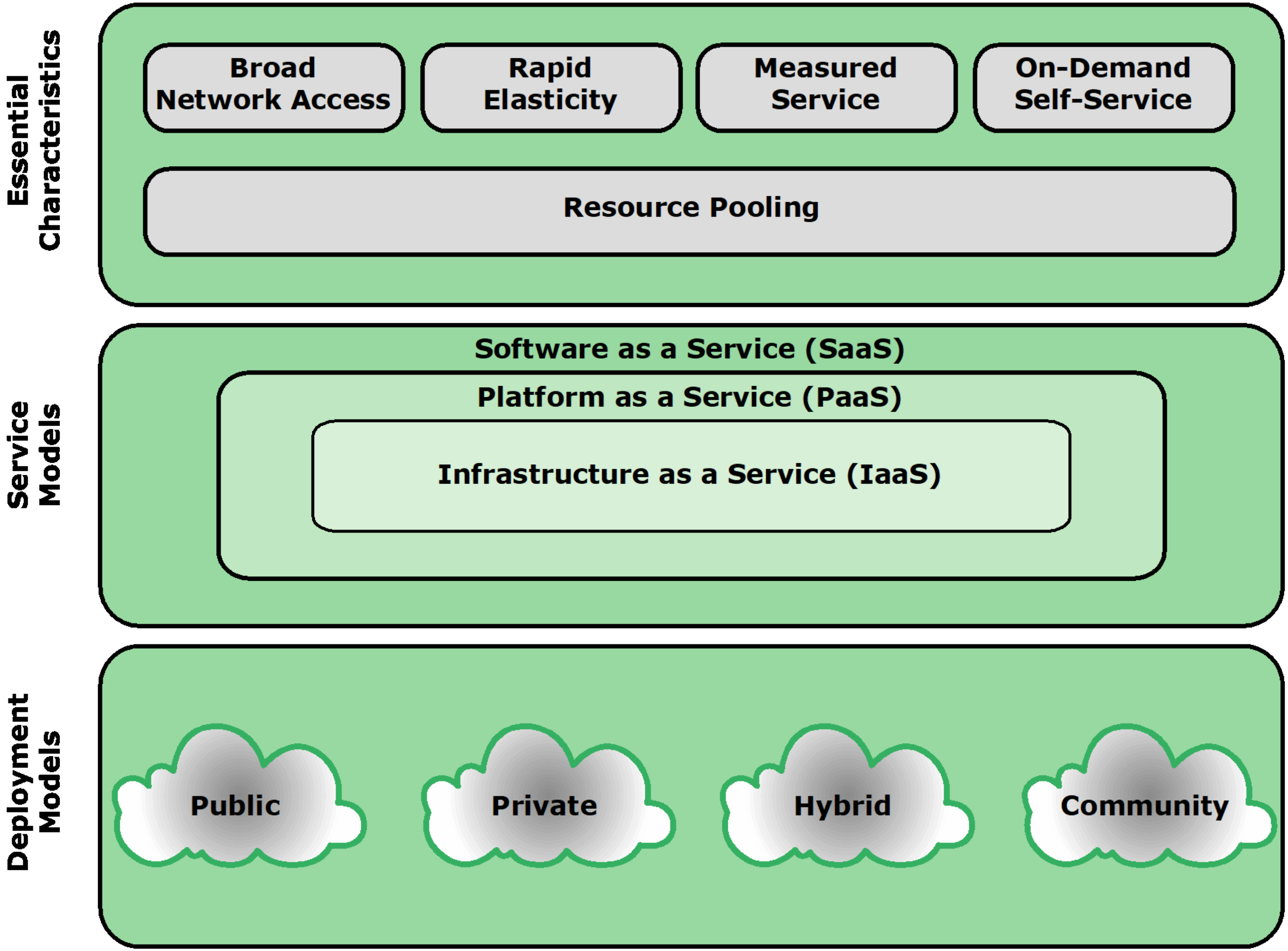


Figure 13.1 Cloud Computing Elements

Cloud Service Models

NIST defines three service models, which can be viewed as nested service alternatives

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

Infrastructure as a Service (IaaS)

With IaaS, the customer has access to the resources of the underlying cloud infrastructure

The cloud service user does not manage or control the resources of the underlying cloud infrastructure, but has control over operating systems, deployed applications, and possibly limited control of select networking components

IaaS provides virtual machines and other virtualized hardware and operating systems

IaaS offers the customer processing, storage, networks, and other fundamental computing resources so the customer is able to deploy and run arbitrary software, which can include operating systems and applications

IaaS enables customers to combine basic computing services, such as number crunching and data storage, to build highly adaptable computer systems

Examples of IaaS are Amazon Elastic Compute Cloud, Microsoft Windows Azure, Google Compute Engine, and Rackspace

Platform as a Service (PaaS)

A PaaS cloud provides service to customers in the form of a platform on which the customer's applications can run

PaaS enables the customer to deploy onto the cloud infrastructure customer-created or acquired applications

A PaaS cloud provides useful software building blocks, plus a number of development tools, such as programming language tools, run-time environments, and other tools that assist in deploying new applications

In effect, PaaS is an operating system in the cloud

It is useful for an organization that wants to develop new or tailored applications while paying for the needed computing resources only as needed, and only for as long as needed

Examples of PaaS include AppEngine, Engine Yard, Heroku, Microsoft Azure, Force.com, and Apache Stratos

Software as a Service (SaaS)

SaaS provides service to customers in the form of software, specifically virtualised application software, running on and accessible in the cloud

It enables the customer to use the cloud provider's applications running on the provider's cloud infrastructure

- The applications are accessible from various client devices through a simple interface, such as a Web browser
- Instead of obtaining desktop and server licenses for software products it uses, an enterprise obtains the same functions from the cloud service

The use of SaaS avoids the complexity of software installation, maintenance, upgrades, and patches

Examples of this service are Google Gmail, Microsoft 365, Salesforce, Citrix GoToMeeting, and Cisco WebEx

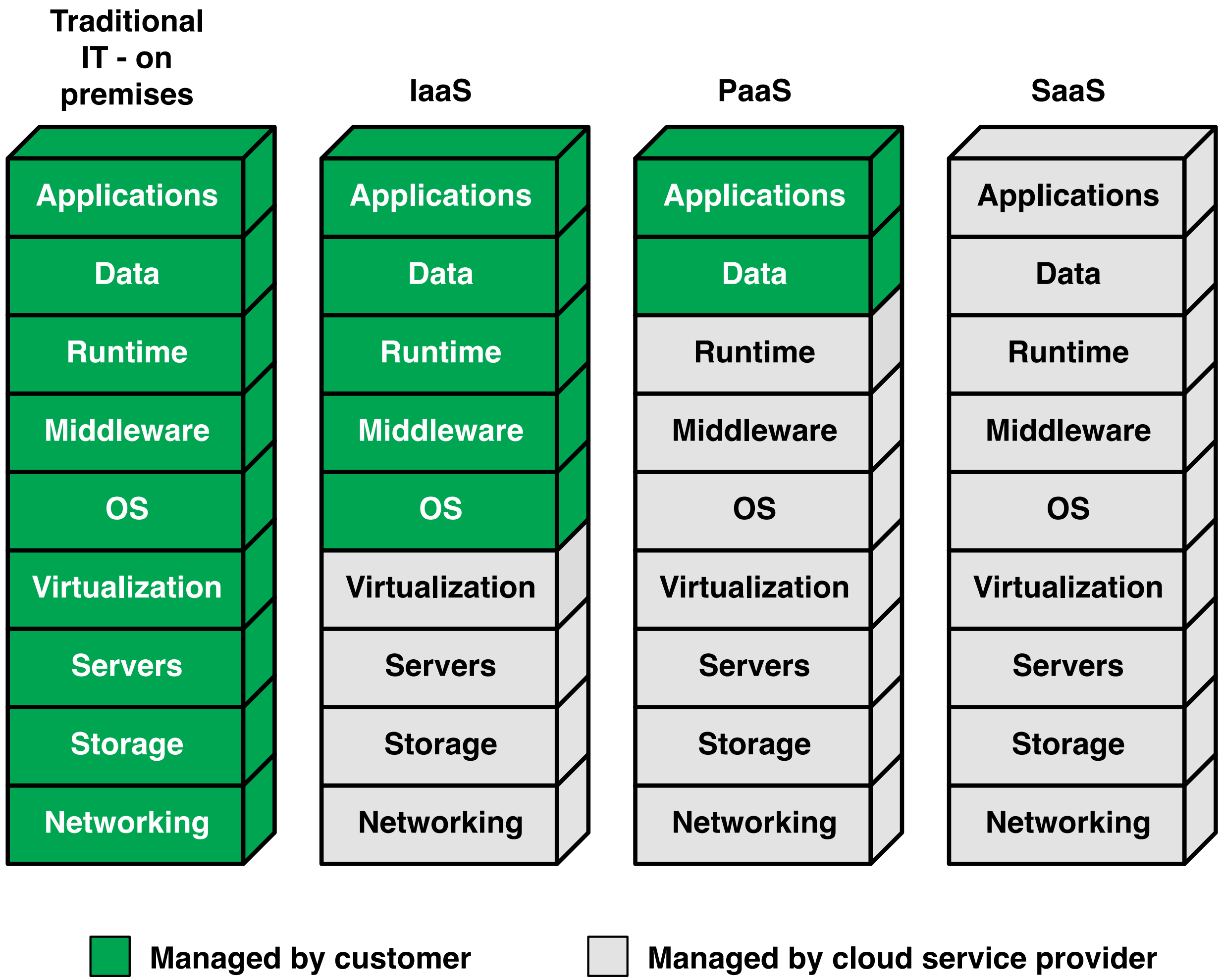


Figure 13.2 Separation of Responsibilities in Cloud Service Models

Cloud Deployment Models

Public cloud

Community cloud

The four most prominent deployment models for cloud computing are:

Private cloud

Hybrid cloud

Public Cloud

- A public cloud infrastructure is made available to the general public or a large industry group, and is owned by an organization selling cloud services
    - The cloud provider is responsible both for the cloud infrastructure and for the control of data and operations within the cloud
- A public cloud may be owned, managed, and operated by a business, academic, or government organization, or some combination of them
    - All major components are outside the enterprise firewall, located in a multitenant infrastructure
    - Applications and storage are made available over the Internet via secured IP, and can be free or offered at a pay-per-usage fee
- The major advantage of the public cloud is cost
- The principal concern is security

Private Cloud

- A private cloud is implemented within the internal IT environment of the organization
- The organization may choose to manage the cloud in house or contract the management function to a third party
- The cloud servers and storage devices may exist on premise or off premise
- Private clouds can deliver IaaS internally to employees or business units, as well as software or storage as services to its branch offices
- Examples of services delivered through the private cloud include database on demand, email on demand, and storage on demand
- A key motivation for opting for a private cloud is security
- Other benefits include easy resource sharing and rapid deployment to organizational entities

Community Cloud

A community cloud shares characteristics of private and public clouds	• Has restricted access like a private cloud • The cloud resources are shared among a number of independent organizations like a public cloud
The organizations that share the community cloud have similar requirements and, typically, a need to exchange data with each other	• An example would be the health care industry
The cloud infrastructure may be managed by the participating organizations or a third party, and may exist on premise or off premise	• In this deployment model, the costs are spread over fewer users than a public cloud so only some of the cost savings potential of cloud computing are realized

Hybrid Cloud

- The hybrid cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability
- With a hybrid cloud solution, sensitive information can be placed in a private area of the cloud, and less sensitive data can take advantage of the benefits of the public cloud
- A hybrid public/private cloud solution can be particularly attractive for smaller business
- Many applications for which security concerns are less can be offloaded at considerable cost savings without committing the organization to moving more sensitive data and applications to the public cloud

	Private	Community	Public	Hybrid
Scalability	Limited	Limited	Very high	Very high
Security	Most secure option	Very secure	Moderately secure	Very secure
Performance	Very good	Very good	Low to medium	Good
Reliability	Very high	Very high	Medium	Medium to high
Cost	High	Medium	Low	Medium

Table 13.1
Comparison of Cloud Deployment Models

Cloud Computing:

- NIST SP-500-292 (*NIST Cloud Computing Reference Architecture)* establishes reference architecture, described as follows:

"The NIST cloud computing reference architecture focuses on the requirements of "what" cloud services provide, not a "how to" design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference."

Objectives

NIST developed the reference architecture with the following objectives in mind:

- To illustrate and understand the various cloud services in the context of an overall cloud computing conceptual model
- To provide a technical reference for cloud users to understand, discuss, categorize, and compare cloud services
- To facilitate the analysis of candidate standards for security, interoperability, and portability and reference implementations

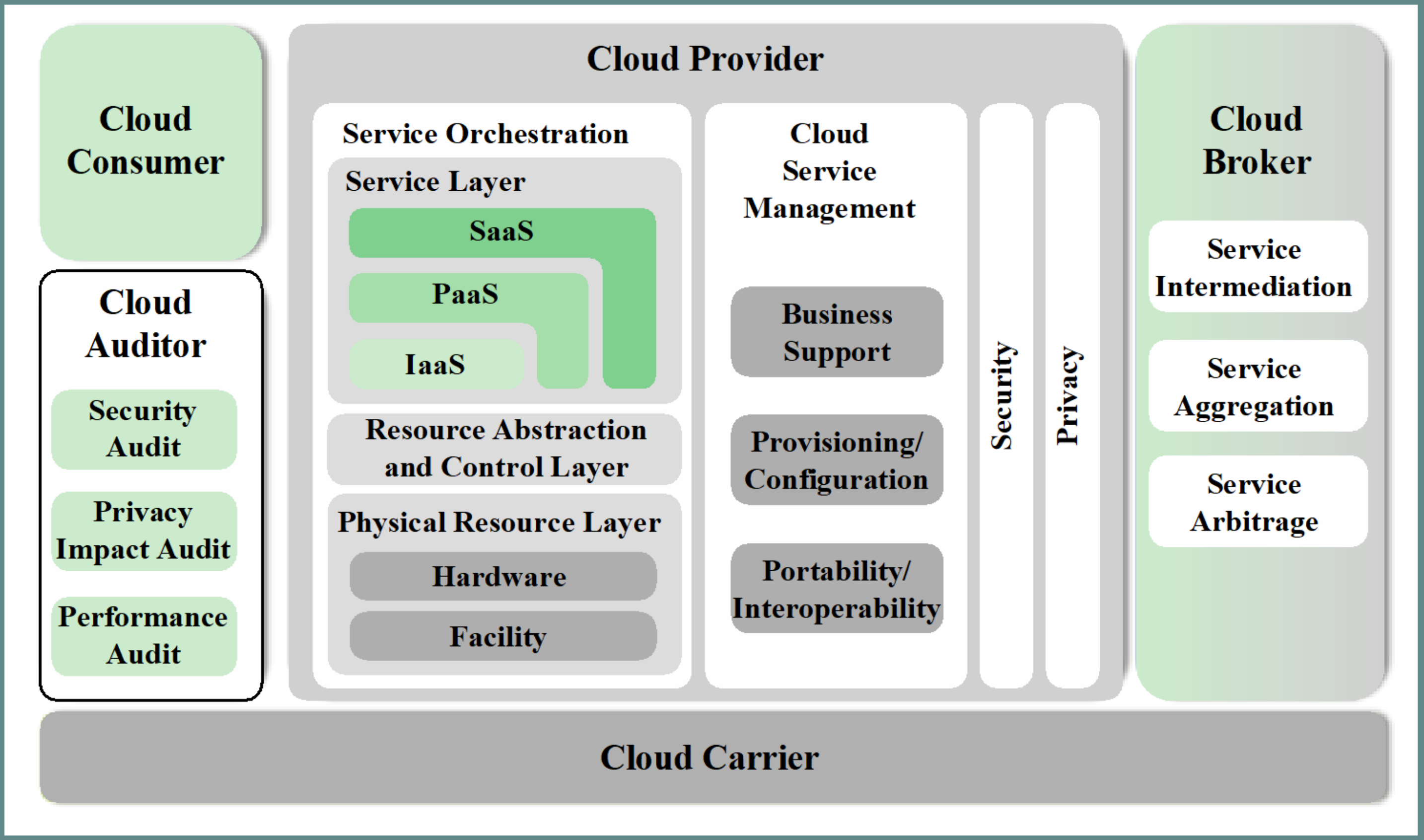


Figure 13.3 NIST Cloud Computing Reference Architecture

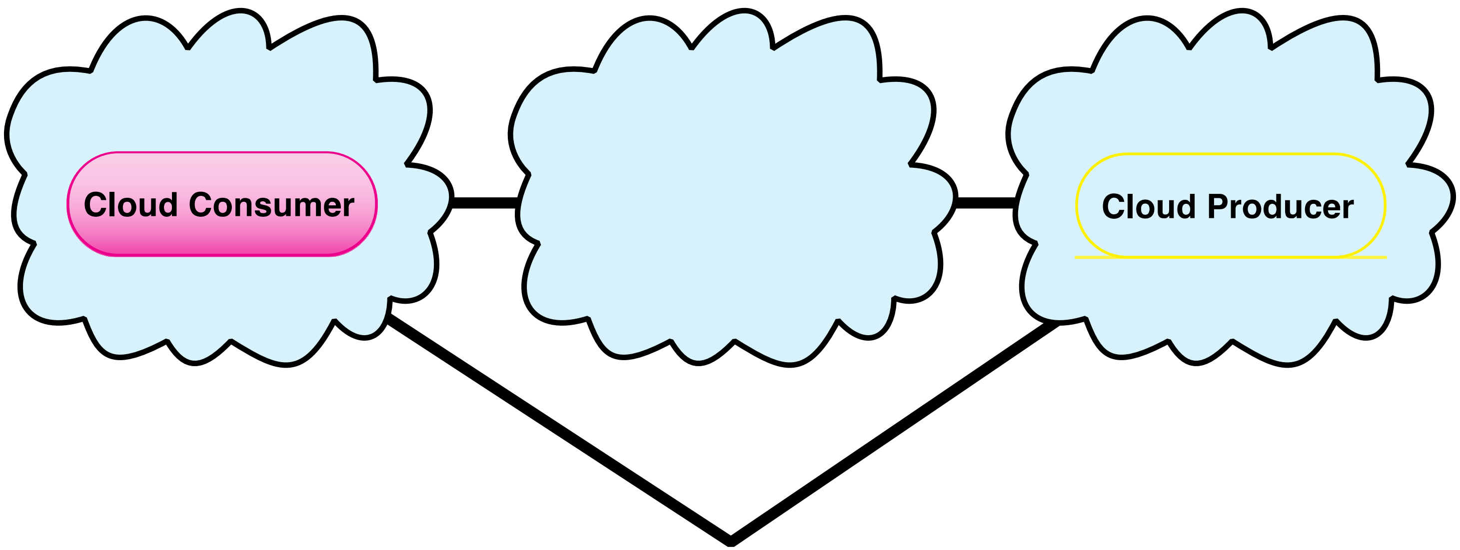


Figure 13.4 Interactions Between Actors in Cloud Computing

Table 13.2 NIST Guidelines on Cloud Security and Privacy Issues and Recommendations SUMMARY

- Governance
- Compliance
- Trust
- Architecture
- Identity and access management
- Software isolation
- Data protection
- Availability
- Incident response

Table 13.2

NIST Guidelines on Cloud Security and Privacy Issues and Recommendations

(Page 1 of 2)

Governance

Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services.

Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.

Compliance

Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements.

Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements.

Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.

Trust

Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time.

Establish clear, exclusive ownership rights over data.

Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system.

Continuously monitor the security state of the information system to support ongoing risk management decisions.

Architecture

Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.

Identity and access management

Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.

Software isolation

Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.

Data protection

Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.

Take into consideration the risk of collating organizational data with those of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value.

Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.

(Table is on pages 433-434 in the textbook)

Availability

Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements.

Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.

Incident response

Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization.

Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.

Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

Table 13.2

NIST Guidelines on Cloud Security and Privacy Issues and Recommendations

(Page 2 of 2)

Security Issues for Cloud Computing

- Security is a major consideration when augmenting or replacing on-premises systems with cloud services
- Allaying security concerns is frequently a prerequisite for further discussions about migrating part or all of an organization's computing architecture to the cloud
- Availability is another major concern
- Auditability of data must be ensured
- Cloud users are often still responsible for application-level security

Security Issues for Cloud Computing

- Cloud vendors are responsible for physical security and some software security
- Security for intermediate layers of the software stack is shared between users and vendors
- Cloud providers must guard against theft or denial-of-service attacks by their users and users need to be protected from one another
- Businesses should consider the extent to which subscribers are protected against the provider, especially in the area of inadvertent data loss

Table 13.3

Control Functions and Classes

Technical	Operational	Management
Access Control Audit and Accountability Identification and Authentication System and Communication Protection	Awareness and Training Configuration and Management Contingency Planning Incident Response Maintenance Media Protection Physical and Environmental Protection Personnel Security System and Information Integrity	Certification, Accreditation and Security Assessment Planning Risk Assessment System and Services Acquisition

Risks and Countermeasures

The Cloud Security Alliance lists the following as the top cloud-specific security threats:

- Abuse and nefarious use of cloud computing
  - Countermeasures include:
    - Stricter initial registration and validation processes
    - Enhanced credit card fraud monitoring and coordination
    - Comprehensive inspection of customer network traffic
    - Monitoring public blacklists for one's own network blocks

Risks and Countermeasures

- Insecure interfaces and APIs
  - Countermeasures include:
    - Analyzing the security model of CSP interfaces
    - Ensuring that strong authentication and access controls are implemented in concert with encrypted transmission
    - Understanding the dependency chain associated with the API

- Malicious insiders
  - Countermeasures include:
    - Enforce strict supply chain management and conduct a comprehensive supplier assessment
    - Specify human resource requirements as part of legal contract
    - Require transparency into overall information security and management practices, as well as compliance reporting
    - Determine security breach notification processes

- Shared technology issues
  - Countermeasures include:
    - Implement security best practices for installation/configuration
    - Monitor environment for unauthorized changes/activity
    - Promote strong authentication and access control for administrative access and operations
    - Enforce SLAs for patching and vulnerability remediation
    - Conduct vulnerability scanning and configuration audits

- Data loss or leakage
  - Countermeasures include:
    - Implement strong API access control
    - Encrypt and protect integrity of data in transit and at rest
    - Analyze data protection at both design and run time
    - Implement strong key generation, storage and management, and destruction practices

- Account or service hijacking
  - Countermeasures include:
    - Prohibit the sharing of account credentials between users and services
    - Leverage strong two-factor authentication techniques where possible
    - Employ proactive monitoring to detect unauthorized activity
    - Understand CSP security policies and SLAs

- Unknown risk profile
  - Countermeasures include:
    - Disclosure of applicable logs and data
    - Partial/full disclosure of infrastructure details
    - Monitoring and alerting on necessary information

Data Protection in the Cloud

The threat of data compromise increases in the cloud, due to challenges unique to the cloud

Data must be secured while at rest, in transit, and in use, and access to the data must be controlled

The client can employ encryption to protect data in transit, though this involves key management responsibilities for the CSP

The client can enforce access control techniques, but the CSP is involved to some extent depending on the service model used

For data at rest, the ideal security measure is for the client to encrypt the database

Corruption and other denial-of-service attacks remain a risk

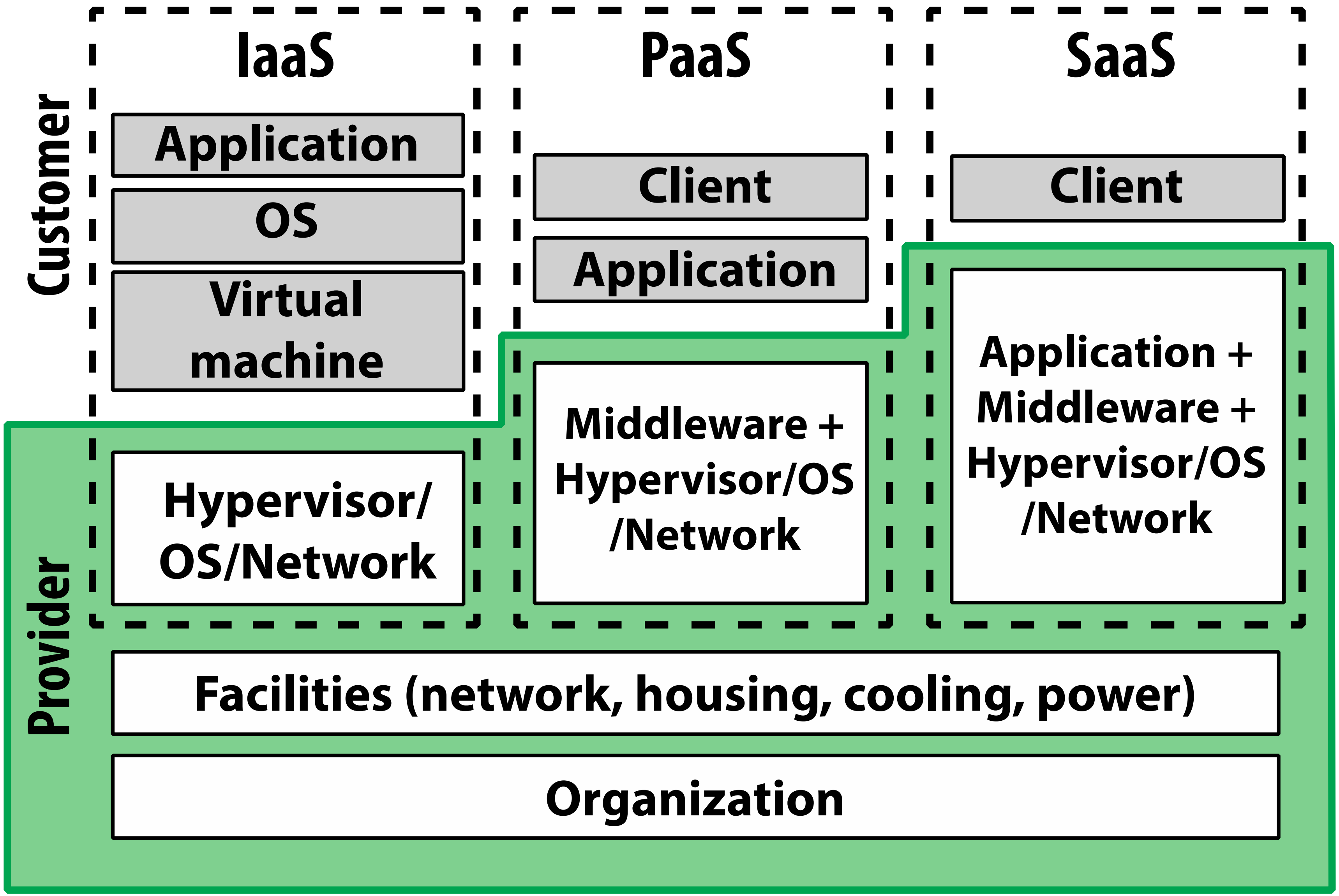
Data Protection in the Cloud

Multi-instance Model

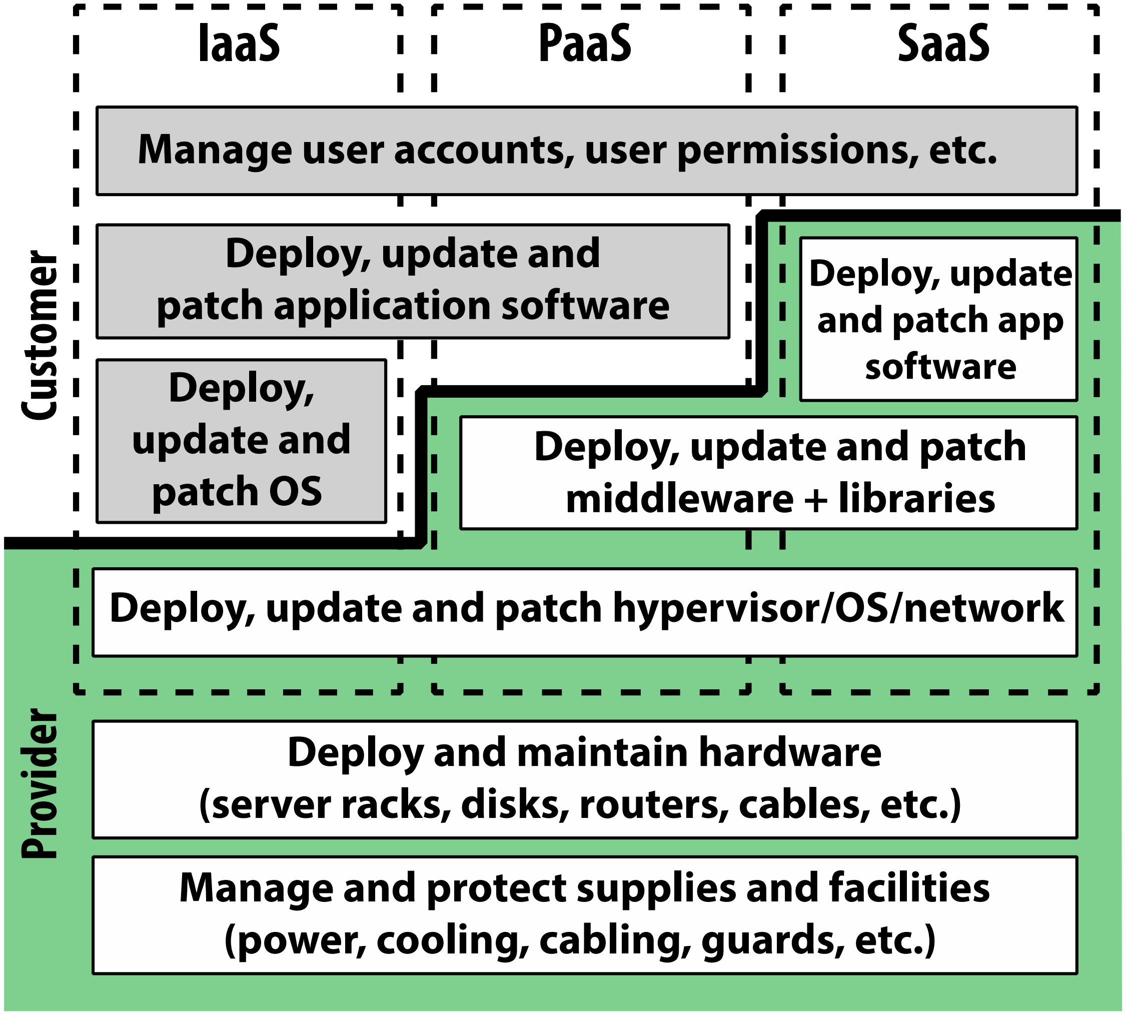
- Provides a uniquely-running VM instance for each cloud subscriber
- This gives the subscriber complete control over role definition, user authorization, and other administrative tasks related to security

Multi-tenant Model

- Provides a predefined environment for the cloud subscriber that is shared with other tenants, typically through tagging data with a subscriber identifier
- Tagging gives the appearance of exclusive use of the instance, but the customer relies on the cloud provider to establish and maintain a sound secure database environment



(a) Cloud computing assets



(b) Cloud computing management tasks

Figure 13.5 Security Considerations for Cloud Computing Assets

Cloud Security as a Service

- In the context of cloud computing, cloud security as a service, designated SecaaS, is a segment of the SaaS offering of a CSP
- The CSA defines SecaaS as the provision of security applications and services via the cloud either to cloud-based infrastructure and software, or from the cloud to the customers' on-premise systems

Cloud Security as a Service

- The CSA has identified the following SecaaS categories of service:
    - Identity and access management
    - Data loss prevention
    - Web security
    - E-mail security
    - Security assessments
    - Intrusion management
    - Security information and event management
    - Encryption
    - Business continuity and disaster recovery
    - Network security

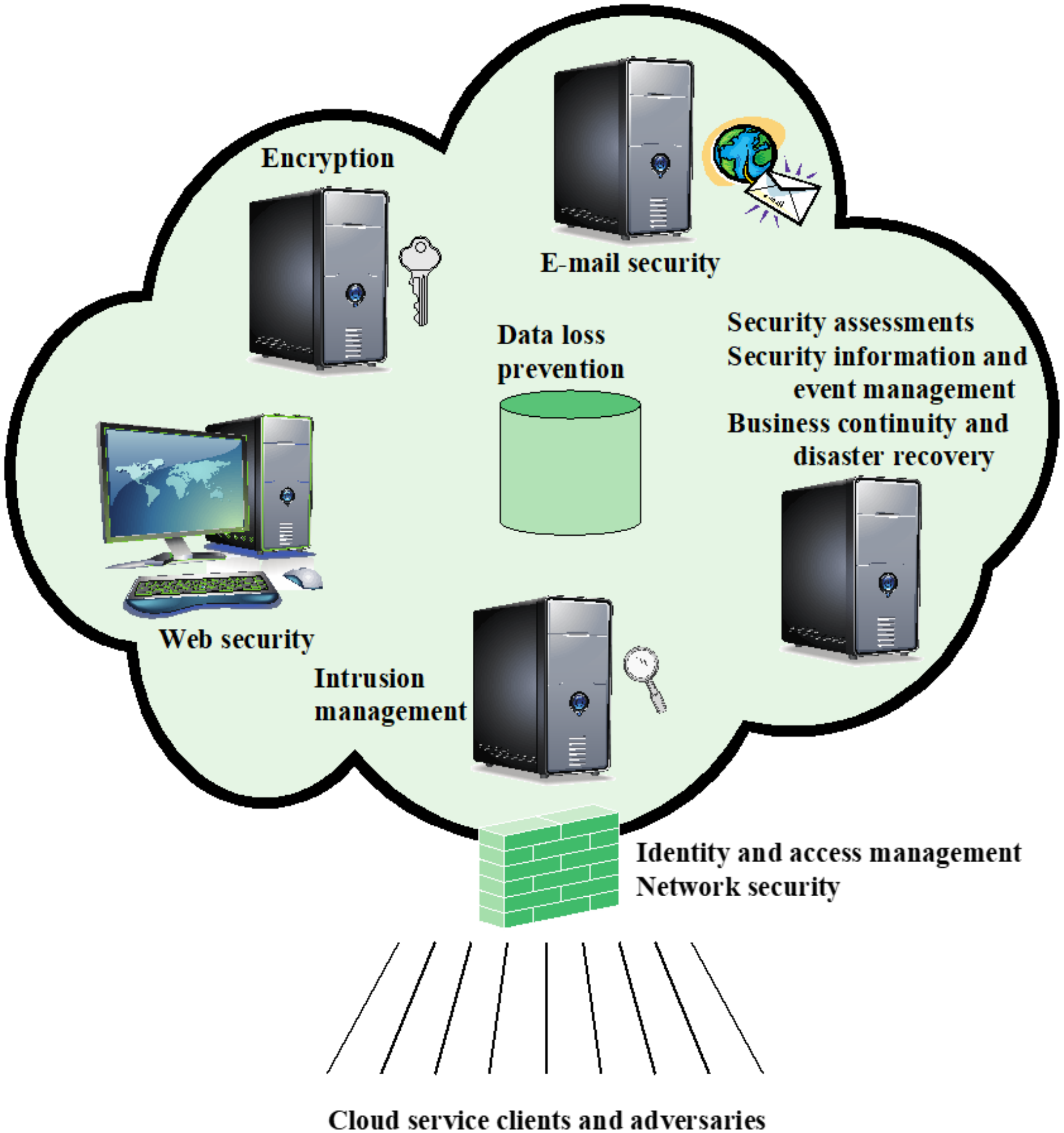


Figure 13.6 Elements of Cloud Security as a Service

OpenStack

Open-source software project of the OpenStack Foundation that aims to produce an open-source cloud operating system

The principal objective is to enable creating and managing huge groups of virtual private servers in a cloud computing environment

OpenStack is embedded, to one degree or another, into data center infrastructure and cloud computing products

It provides multi-tenant IaaS, and aims to meet the needs of public and private clouds, regardless of size, by being simple to implement and massively scalable

OpenStack

- The OpenStack OS consists of a number of independent modules, each of which has a project name and a functional name
- The security module for OpenStack is called Keystone
- Keystone provides the shared security services essential for a functioning cloud computing infrastructure
  - It provides the following main services:
    - Identity
    - Token
    - Service catalog
    - Policies

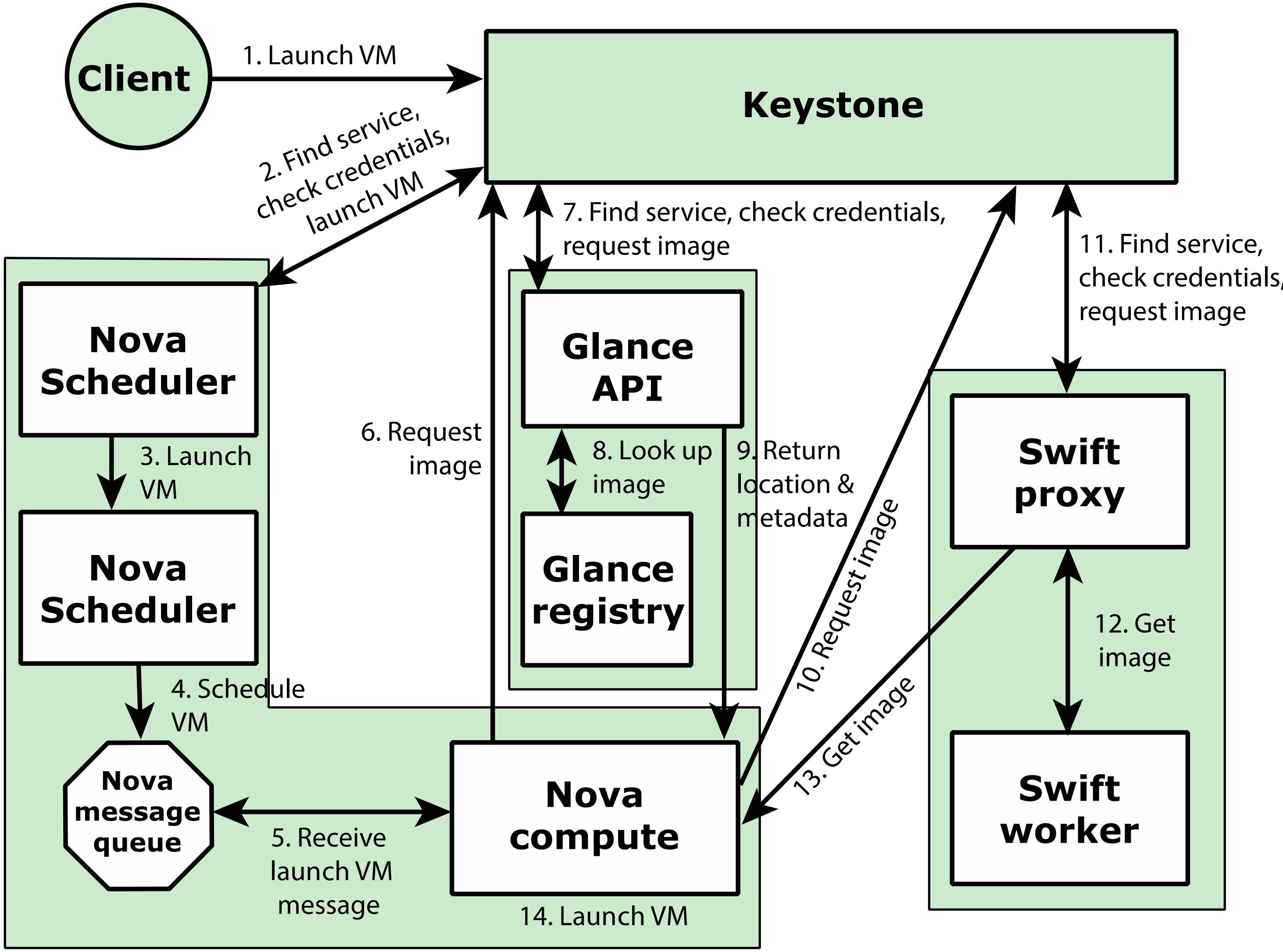


Figure 13.7 Launching a Virtual Machine in OpenStack

The Internet of Things (IoT)

- IoT is a term that refers to the expanding interconnection of smart devices, ranging from appliances to tiny sensors
    - Communication between people and things, and between things themselves
    - The Internet supports the interconnectivity usually through cloud systems
- The objects deliver sensor information, act on their environment, and in some cases modify themselves, to create overall management of a larger system
- The IoT is primarily driven by deeply embedded devices
    - These devices are low-bandwidth, low-repetition data capture, and low-bandwidth data-usage appliances that communicate with each other and provide data via user interfaces
    - Embedded appliances, such as high-resolution video security cameras, video VoIP phones, and a handful of others, require high-bandwidth streaming capabilities

Evolution

With reference to the end systems supported, the Internet has gone through roughly four generations of deployment culminating in the IoT:

Information technology (IT)	PCs, servers, routers, firewalls, and so on, bought as IT devices by enterprise IT people, primarily using wired connectivity
Operational technology (OT)	Machines/appliances with embedded IT built by non-IT companies, such as medical machinery, SCADA, process control, and kiosks, bought as appliances by enterprise OT people, primarily using wired connectivity
Personal technology	Smartphones, tablets, and eBook readers bought as IT devices by consumers (employees) exclusively using wireless connectivity and often multiple forms of wireless connectivity
Sensor/actuator technology	Single-purpose devices bought by consumers, IT and OT people exclusively using wireless connectivity, generally of a single form, as part of larger systems

It is the fourth generation that is usually thought of as the IoT, and which is marked by the use of billions of embedded devices

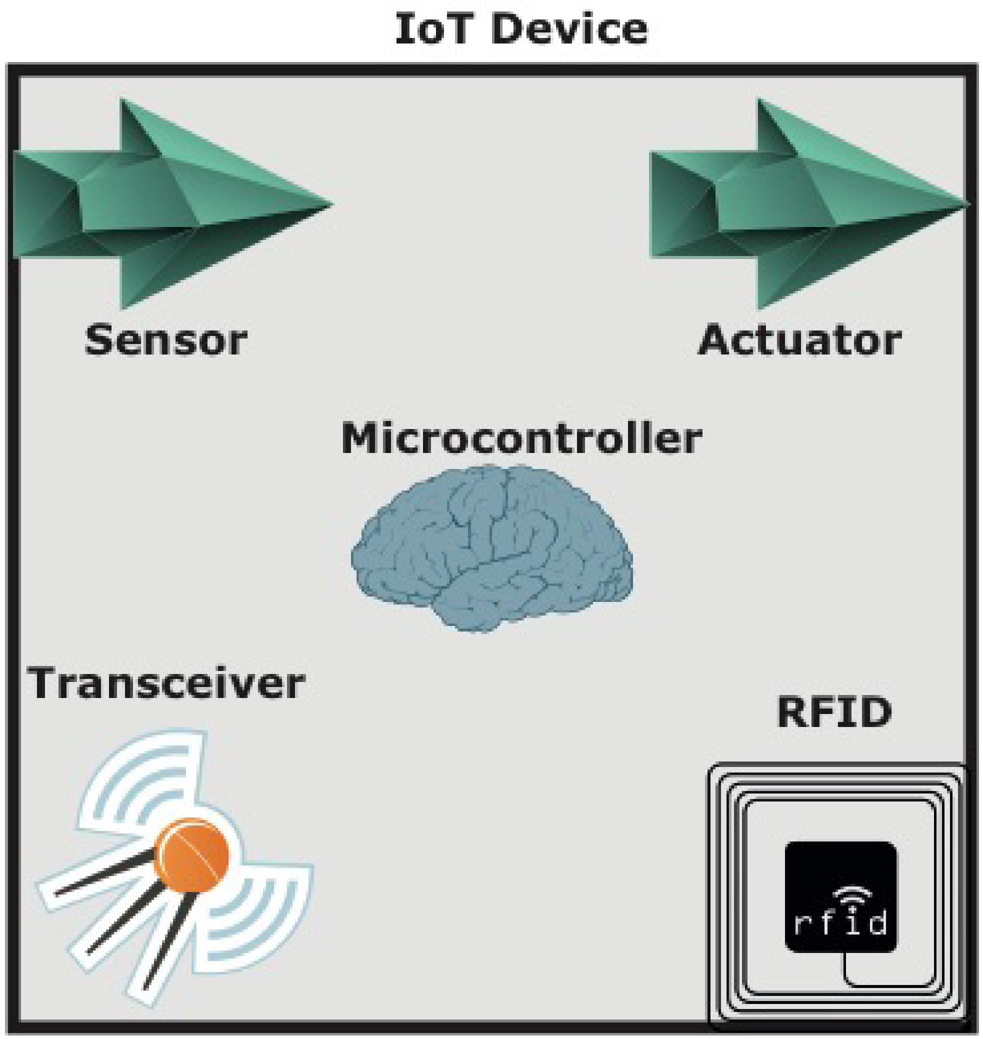


Figure 13.8 IoT Components

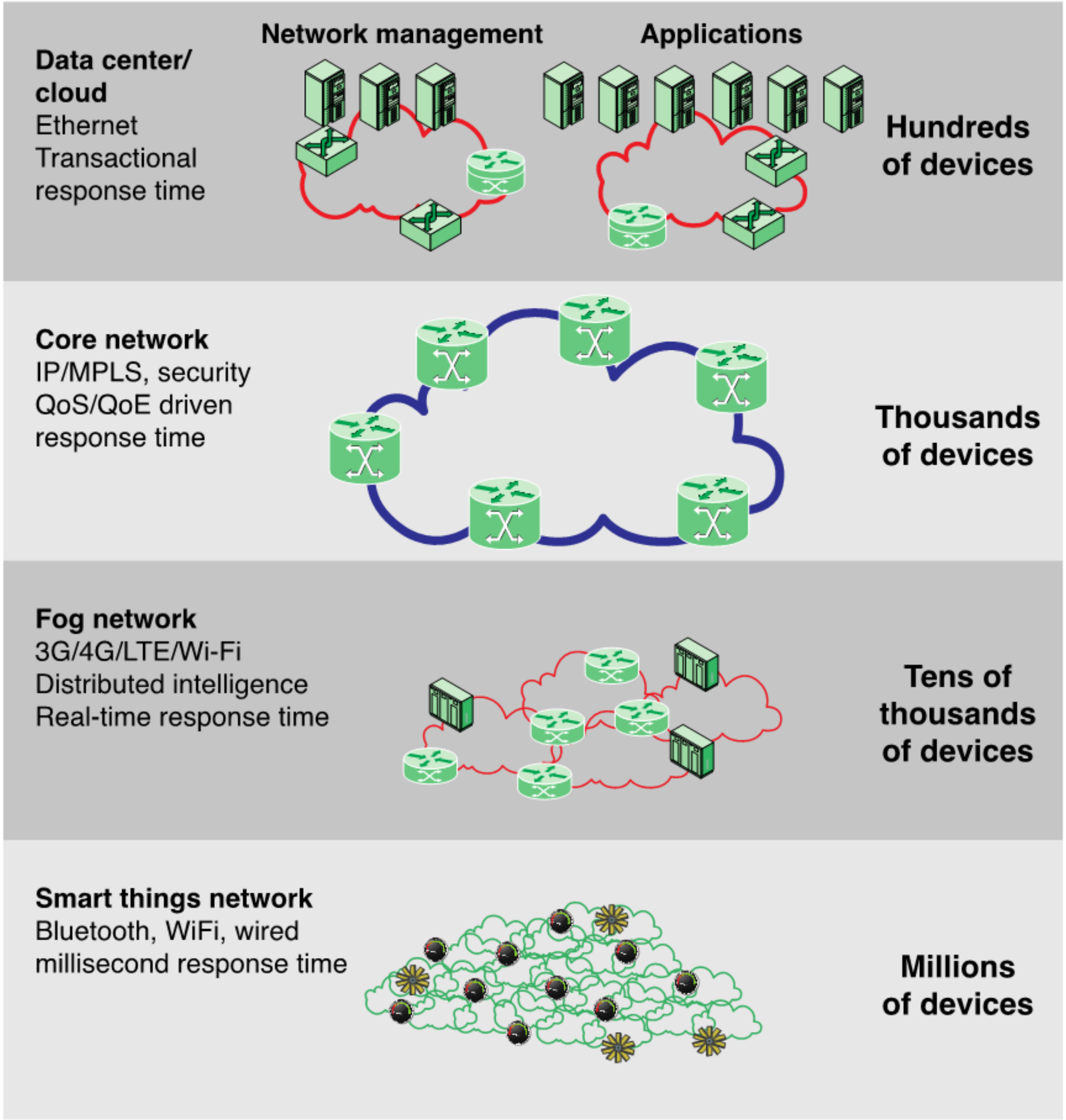


Figure 13.9 The IoT/Cloud Context

Edge

At the edge of a typical enterprise network is a network of IoT-enabled devices consisting of sensors and perhaps actuators

- These devices may communicate with one another
- A cluster of sensors may all transmit their data to one sensor that aggregates the data to be collected by a higher-level entity

A *gateway* interconnects the IoT-enabled devices with the higher-level communication networks

- It performs the necessary translation between the protocols used in the communication networks and those used by devices
- It may also perform a basic data aggregation function

Fog

- In many IoT deployments, massive amounts of data may be generated by a distributed network of sensors
- Rather than store all of that data permanently (or at least for a long period) in central storage accessible to IoT applications, it is often desirable to do as much data processing close to the sensors as possible
- The purpose of what is sometimes referred to as the edge computing level is to convert network data flows into information that is suitable for storage and higher-level processing
- Processing elements at these levels may deal with high volumes of data and perform data transformation operations, resulting in the storage of much lower volumes of data
- The following are examples of fog computing operations:

Evaluation	Formatting	Expanding/decoding	Distillation/reduction	Assessment

Fog

- Generally fog computing devices are deployed physically near the edge of the IoT network near the sensors and other data-generating devices
- Fog computing and fog services are expected to be a distinguishing characteristic of the IoT
- Fog computing represents an opposite trend in modern networking from cloud computing
    - With cloud computing, massive, centralized storage and processing resources are made available to distributed customers over cloud networking facilities to a relatively small number of users
    - With fog computing, massive numbers of individual smart objects are interconnected with fog networking facilities that provide processing and storage resources close to the edge devices in an IoT
- Fog computing addresses the challenges raised by the activity of thousands or millions of smart devices, including security, privacy, network capacity constraints, and latency requirements
- The term *fog computing* is inspired by the fact that fog tends to hover low to the ground, whereas clouds are high in the sky

Core

- The *core network,* also referred to as a *backbone network,* connects geographically dispersed fog networks as well as providing access to other networks that are not part of the enterprise network
- Typically the core network will use very high-performance routers, high-capacity transmission lines, and multiple interconnected routers for increased redundancy and capacity
- The core network may also connect to high-performance, high-capacity servers such as large database servers and private cloud facilities
- Some of the core routers may be purely internal, providing redundancy and additional capacity without serving as edge routers

	Cloud	Fog
Location of processing/storage resources	Center	Edge
Latency	High	Low
Access	Fixed or wireless	Mainly wireless
Support for mobility	Not applicable	Yes
Control	Centralized/hierarchical (full control)	Distributed/hierarchical (partial control)
Service access	Through core	At the edge/on handheld device
Availability	99.99%	Highly volatile/highly redundant
Number of users/devices	Tens/hundreds of millions	Tens of billions
Main content generator	Human	Devices/sensors
Content generation	Central location	Anywhere
Content consumption	End device	Anywhere
Software virtual infrastructure	Central enterprise servers	User devices

Table 13.4: Comparison of Cloud and Fog Features

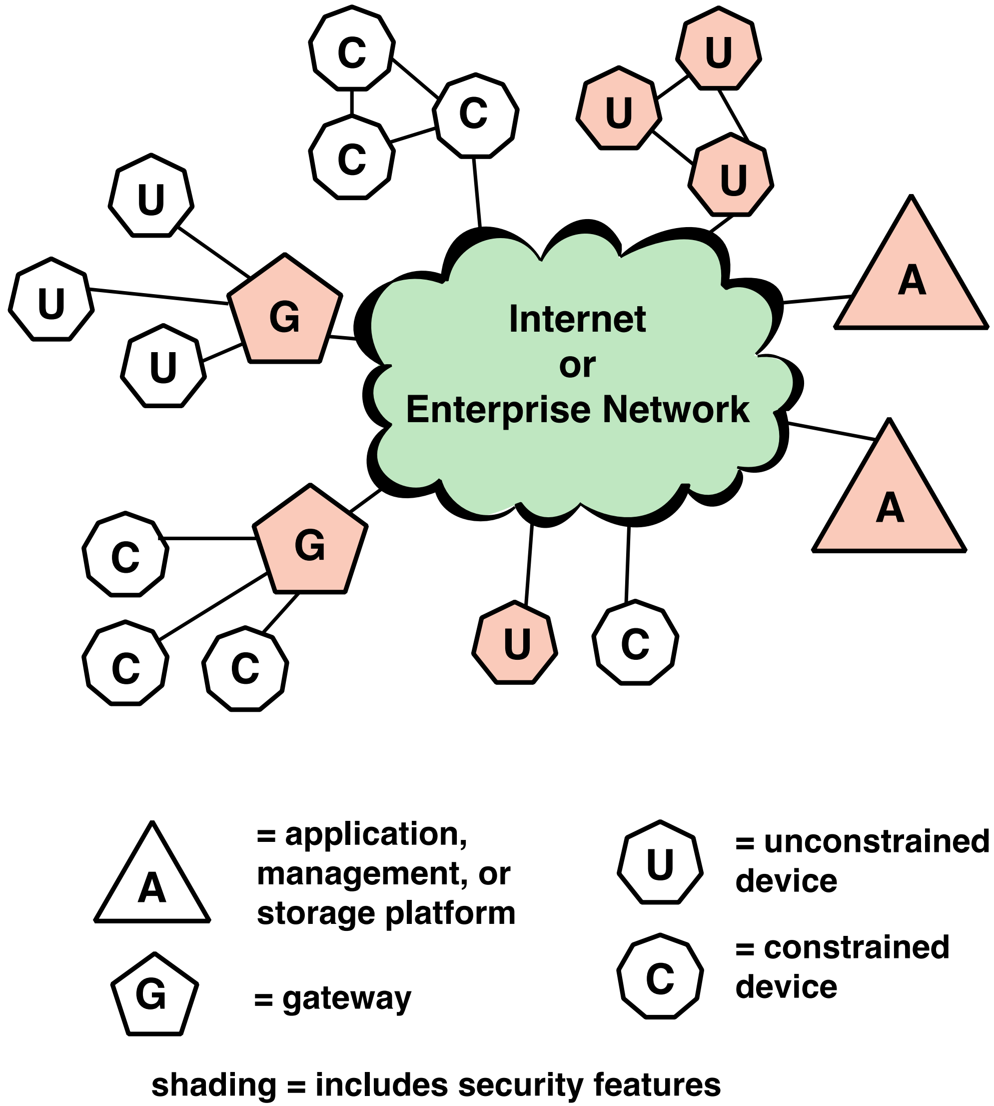


Figure 13.10 IoT Security: Elements of Interest

Patching Vulnerability

There is a crisis point with regard to the security of embedded systems, including IoT devices

The embedded devices are riddled with vulnerabilities and there is no good way to patch them

Chip manufacturers have strong incentives to produce their product as quickly and cheaply as possible

The device manufacturers focus is the functionality of the device itself

The end user may have no means of patching the system or, if so, little information about when and how to patch

The result is that the hundreds of millions of Internet-connected devices in the IoT are vulnerable to attack

This is certainly a problem with sensors, allowing attackers to insert false data into the network

It is potentially a graver threat with actuators, where the attacker can affect the operation of machinery and other devices

IoT Security and Privacy Requirements

- ITU-T Recommendation Y.2066 includes a list of security requirements for the IoT
- The requirements are defined as being the functional requirements during capturing, storing, transferring, aggregating, and processing the data of things, as well as to the provision of services which involve things
- The requirements are:
  - Communication security
  - Data management security
  - Service provision security
  - Integration of security policies and techniques
  - Mutual authentication and authorization
  - Security audit

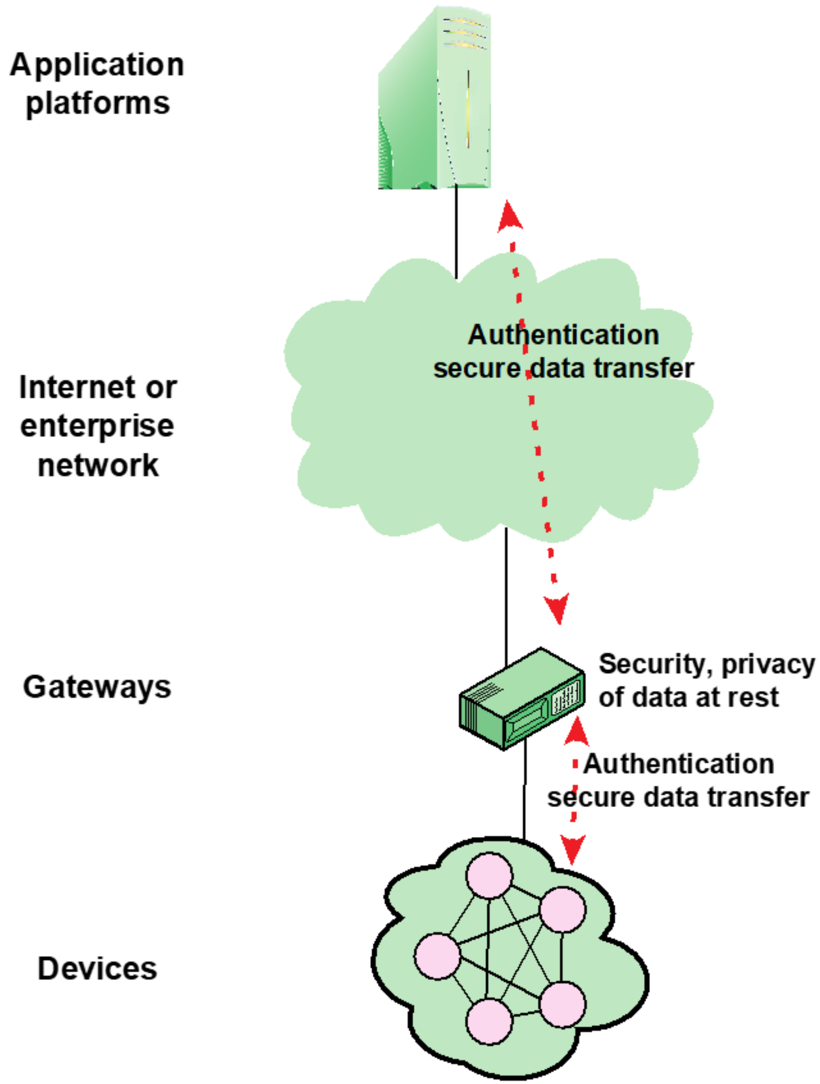


Figure 13.11 IoT Gateway Security Functions

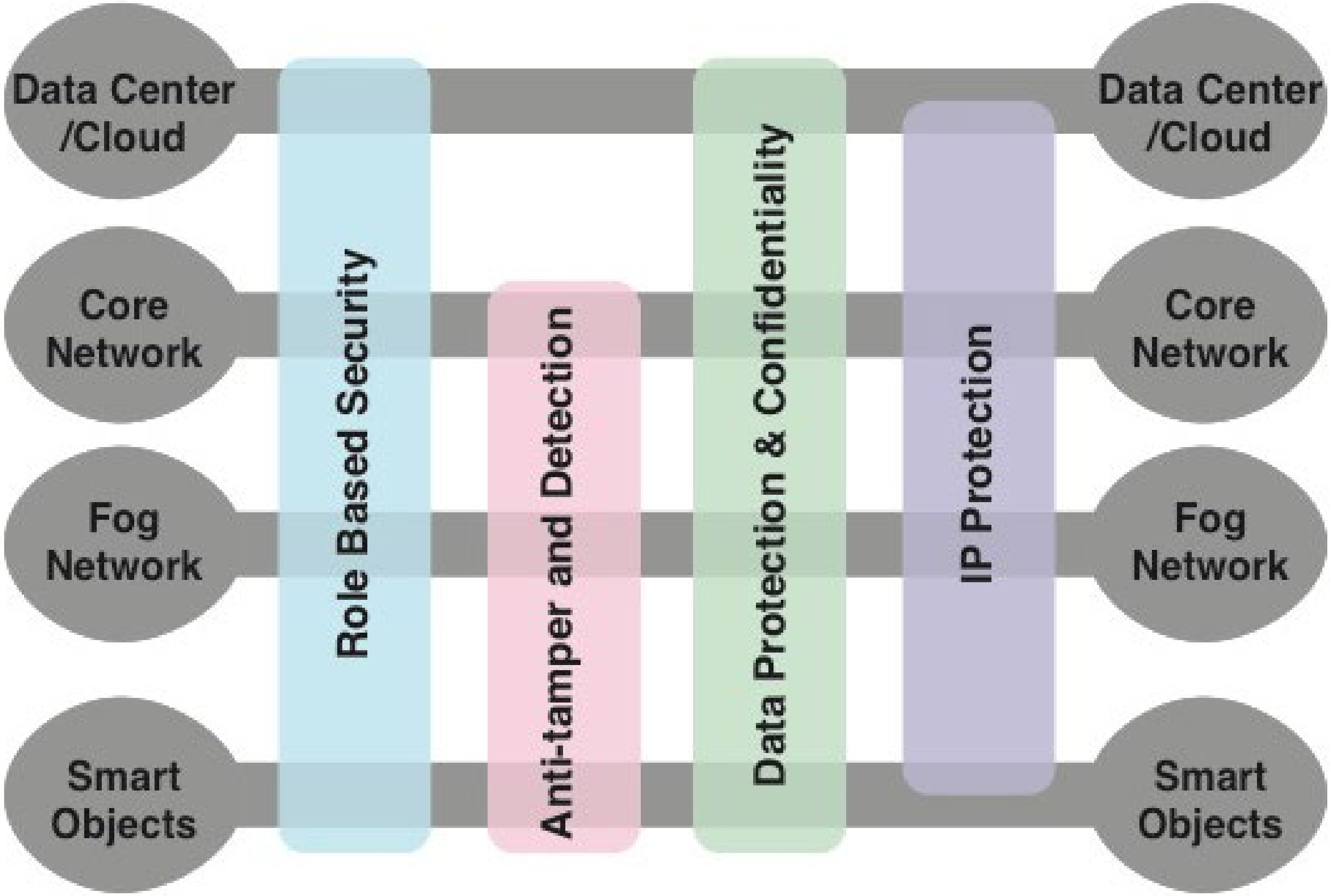


Figure 13.12 IoT Security Environment

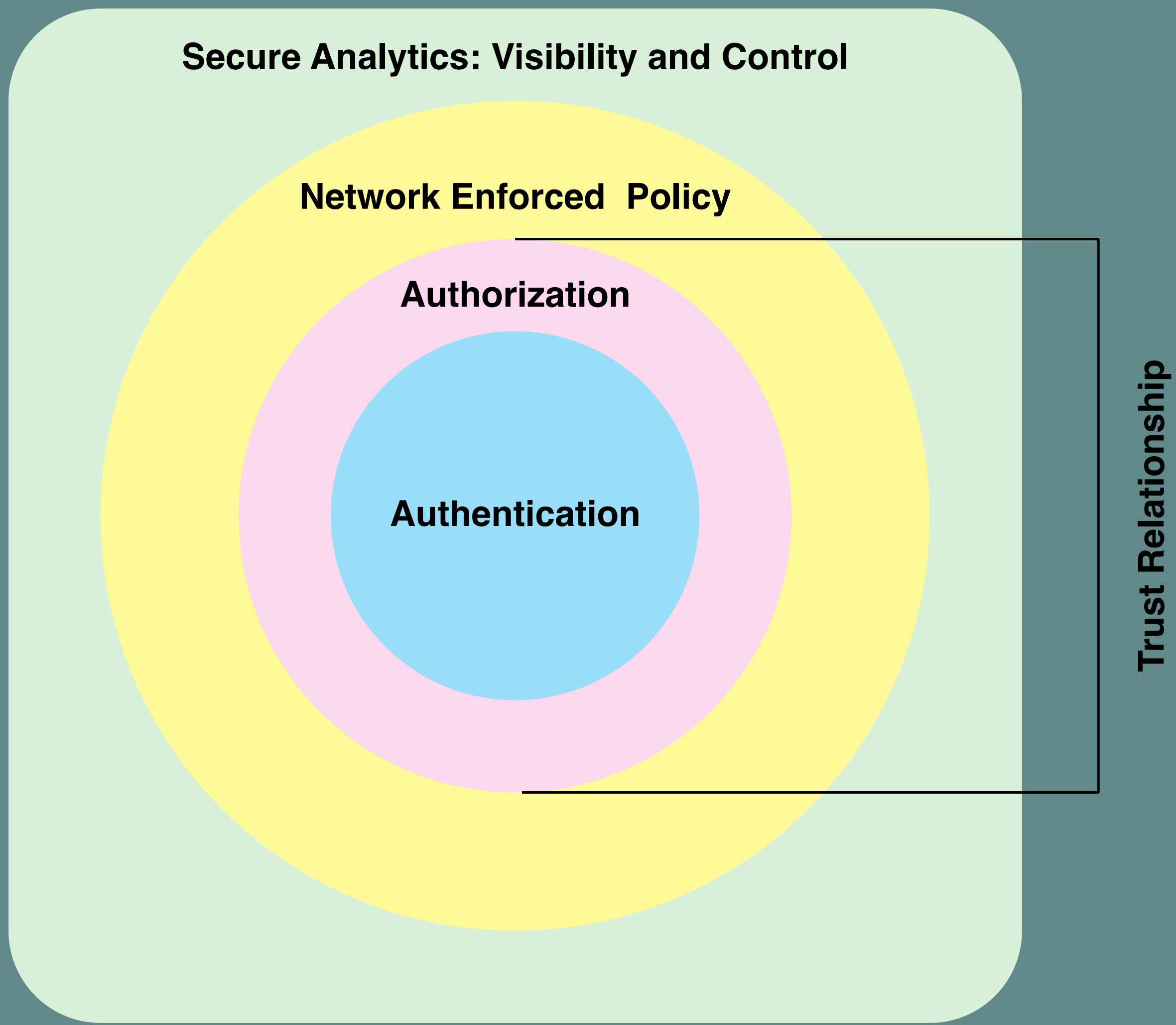


Figure 13.13 Secure IoT Framework

MiniSec

- MiniSec is an open-source security module that is part of the TinyOS operating system
- It is designed to be a link-level module that offers a high level of security, while simultaneously keeping energy consumption low and using very little memory
- MiniSec provides confidentiality, authentication, and replay protection
- MiniSec has two operating modes, one tailored for single-source communication, and another tailored for multi-source broadcast communication

MiniSec

MiniSec is designed to meet the following requirements:

- Data authentication
- Confidentiality
- Replay protection
- Freshness (message age)
- Low energy overhead
- Resilient to lost messages

Summary

- Cloud computing
  - Cloud computing elements
  - Cloud service models
  - Cloud deployment models
  - Cloud computing reference architecture
- Cloud security approaches
  - Risks and countermeasures
  - Data protection in the cloud
  - Security approaches for cloud computing assets
  - Cloud security as a service
  - Open-source cloud security module
- Cloud security concepts
  - Security issues for cloud computing
  - Addressing cloud computing security concerns
- The Internet of Things
  - Things on the Internet of Things
  - Evolution
  - Components of IoT-enabled things
  - IoT and cloud context
- IoT security
  - The patching vulnerability
  - IoT security and privacy requirements defined by ITU-T
  - An IoT security framework
  - An open-source IoT security module