Module 5
Cloud Computing Security

Submodule 2: Cloud Security

NIST Guidelines on Cloud Security

- NIST SP 800-144:
  - Governance
  - Compliance
  - Trust
  - Architecture
  - Identify and access management
  - Software isolation
  - Data protection
  - Availability
  - Incident response

Security Issues of Cloud-I

- 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

Security Issues of Cloud-II

- Businesses should perform due diligence on security threats both from outside and inside the cloud
  - Cloud users are responsible for application-level security
  - 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

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
- 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

Risks and Countermeasures (cont.)

- 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

Risks and Countermeasures (cont.)

- 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

Risks and Countermeasures (cont.)

- 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-I

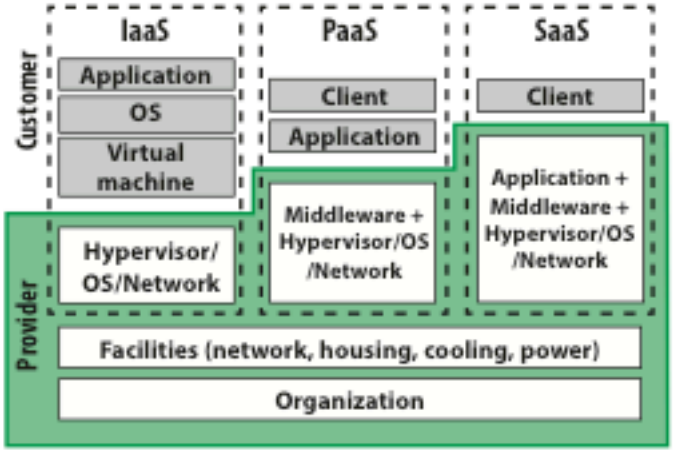
- The threat of data compromise increases in the cloud, due to the number of, and interactions between, risks and challenges that are either unique to the cloud or more dangerous because of the architectural or operational characteristics of the cloud environment
- Data must be secured while at rest, 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

Data Protection in the Cloud-I

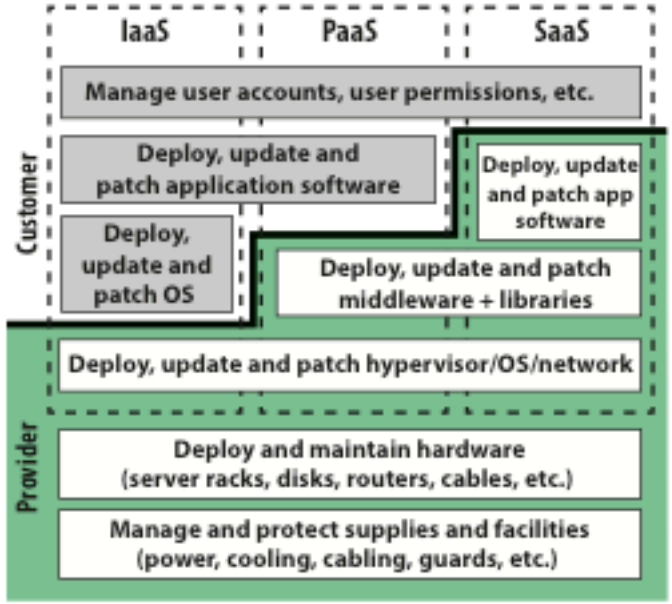
- The client can enforce access control techniques, but CSP is involved to some extent depending on the service model used
- For data at rest, the ideal security measure is for the client to encrypt the database and only store encrypted data in the cloud, with the CSP having no access to the encryption key
- Even with these precautions, corruption and other denial-of-service attacks remain a risk

Data Protection in the Cloud

- Multi-instance Model
  - Provides a unique DBMS running on a 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 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 (Cont.)

- 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

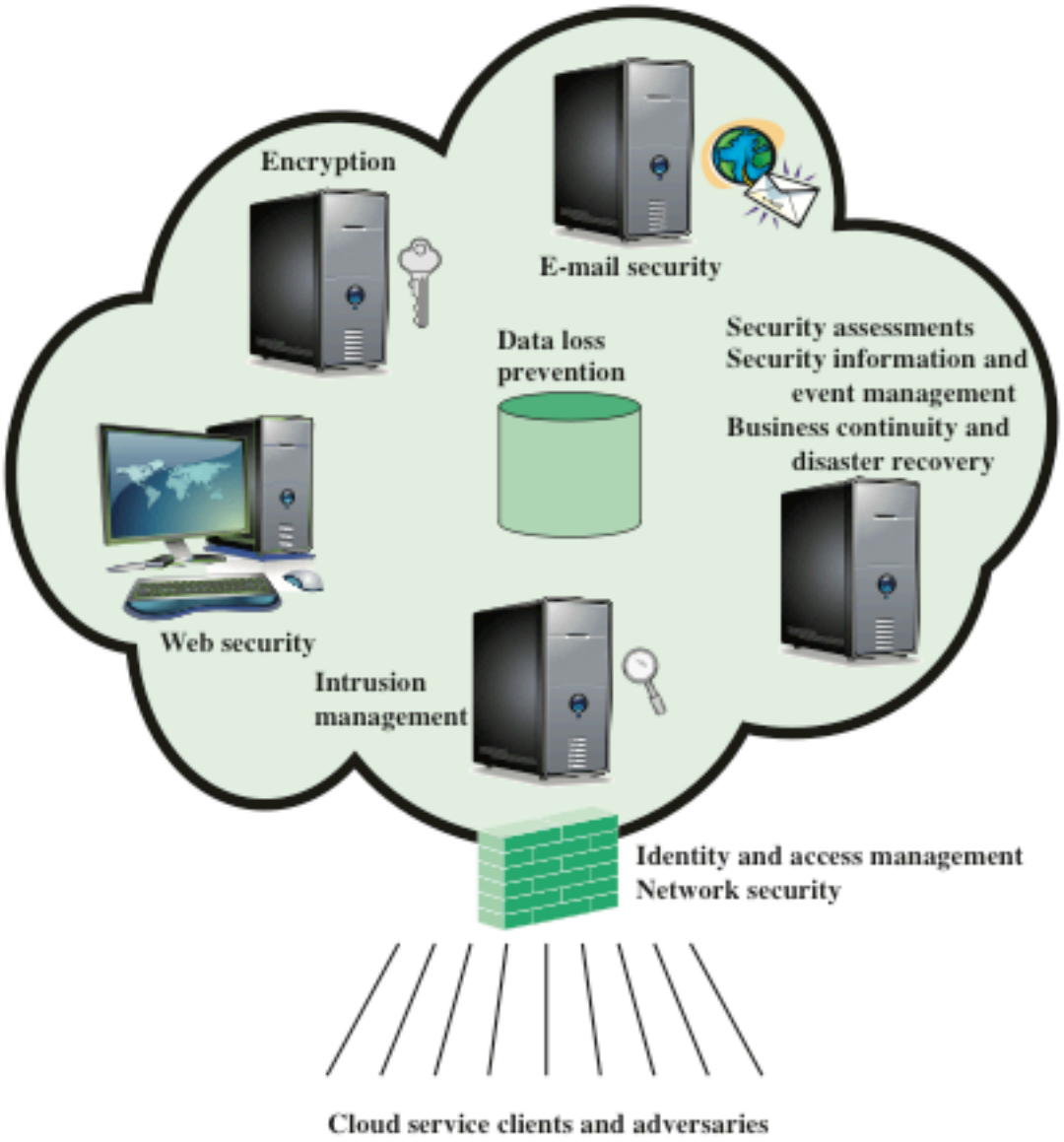


Figure 13.6 Elements of Cloud Security as a Service

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 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

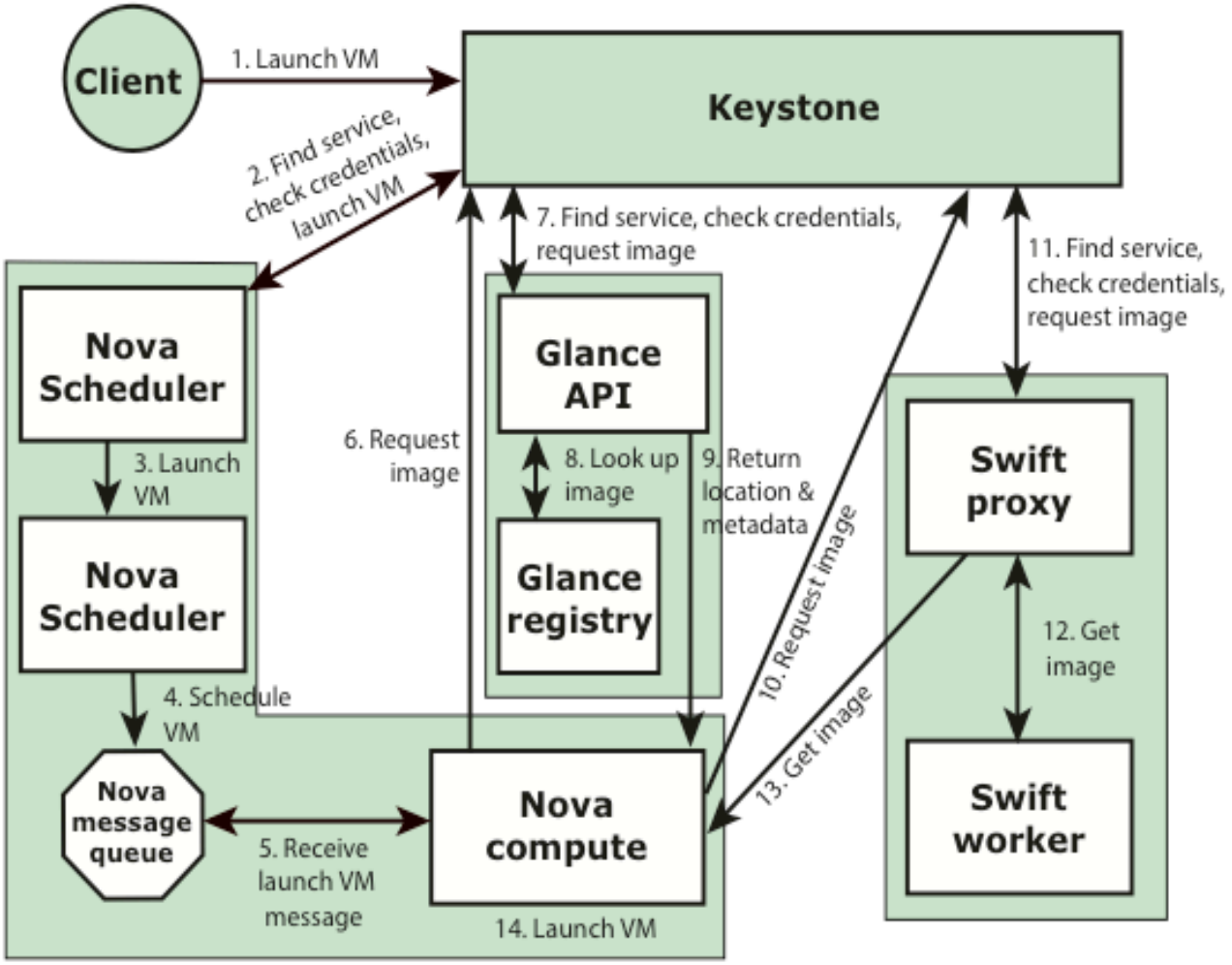


Figure 13.7 Launching a Virtual Machine in OpenStack

The Internet of Things (IoT)

- IoT is a term that refers to the expanding interconnection of smart devices, ranging from appliances to tiny sensors
  - A dominant theme is the embedding of short-range mobile transceivers into a wide array of gadgets and everyday items, enabling new forms of 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 Internet of Things (IoT) (Cont.)

- 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

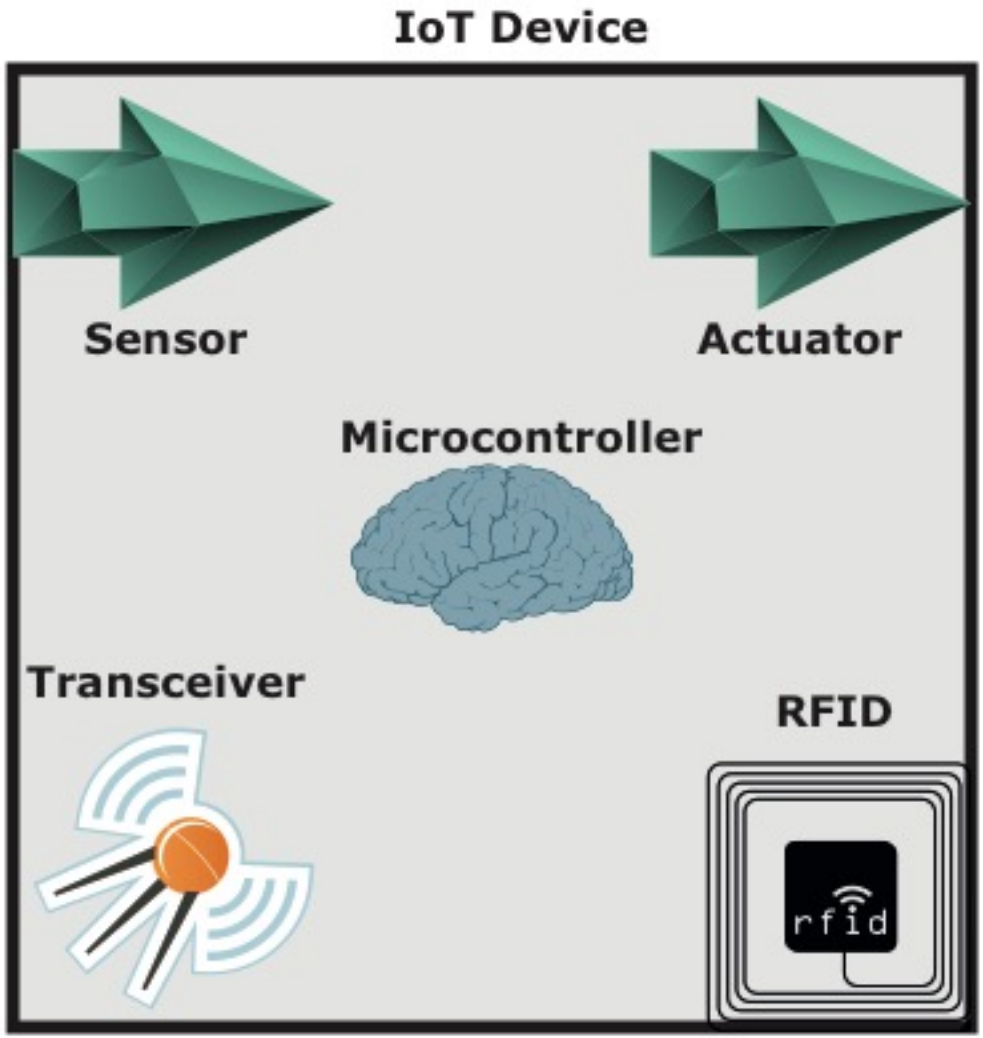


Figure 13.8 IoT Components

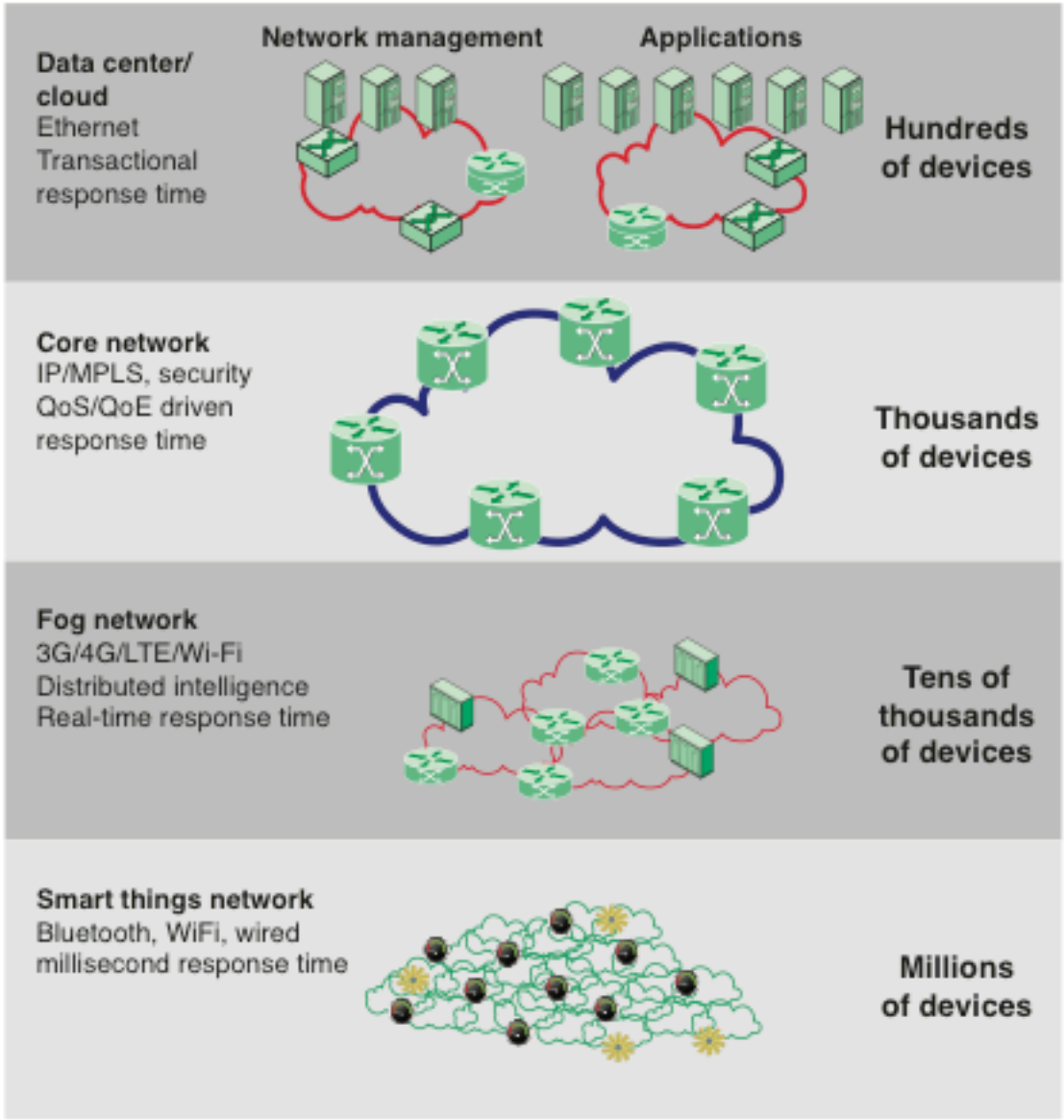


Figure 13.9 The IoT/Cloud Context

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

Fog (Cont.)

- 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 Computing

- 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 (Cont.)

- 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

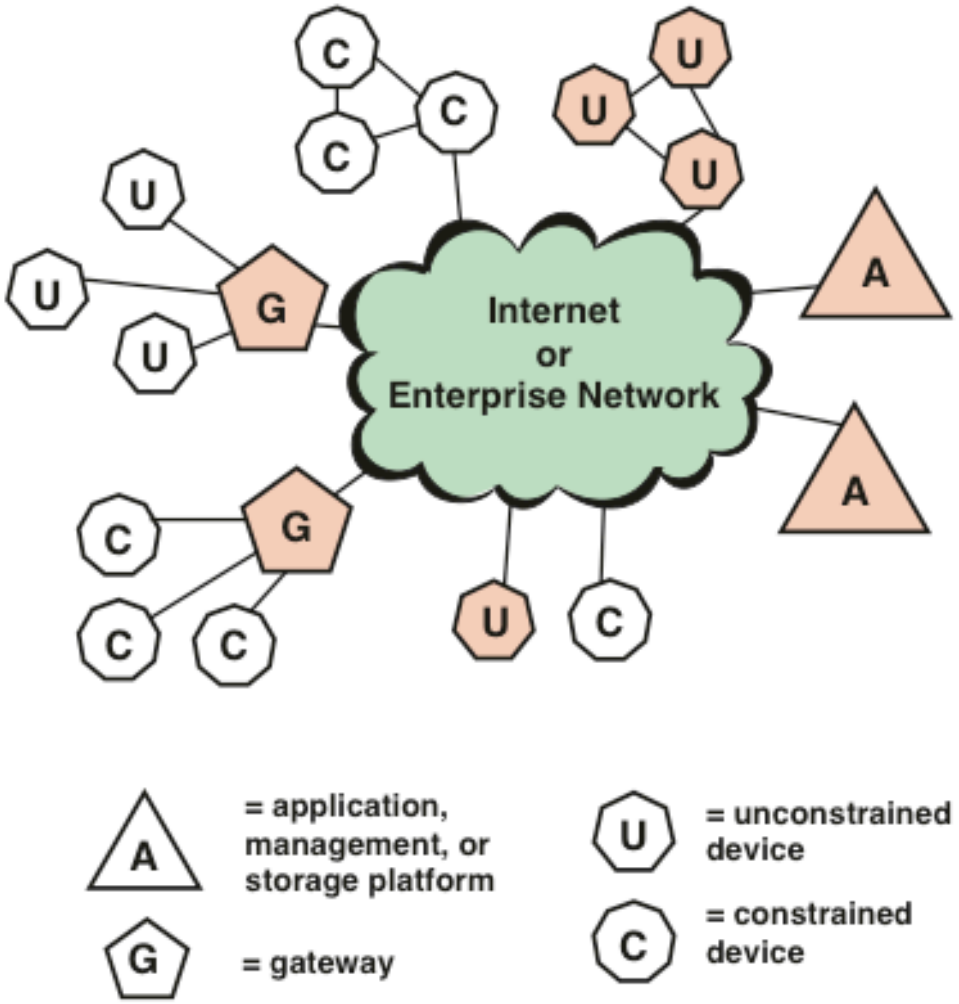


Figure 13.10 IoT Security: Elements of Interest

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

Patching Vulnerability (Cont.)

- 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

IoT Security and Privacy Requirements (Cont.)

- The requirements are:
  - Communication security
  - Data management security
  - Service provision security
  - Integration of security policies and techniques
  - Mutual authentication and authorization
  - Security audit

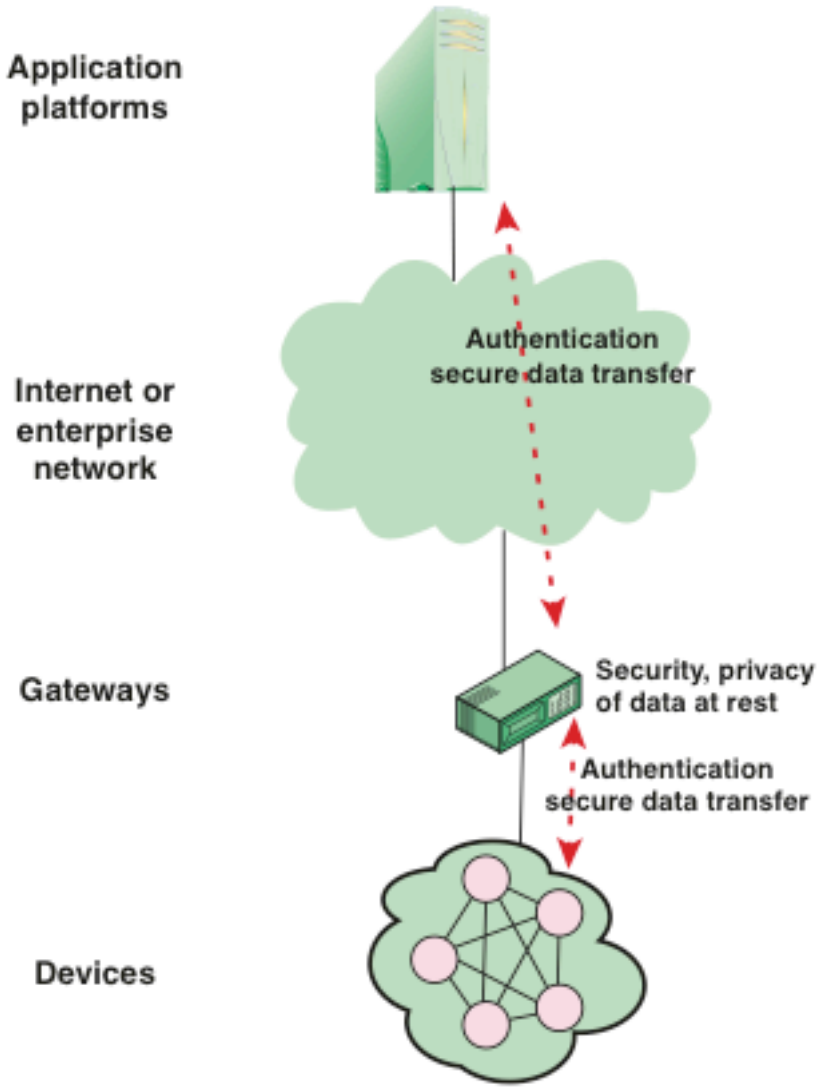


Figure 13.11 IoT Gateway Security Functions

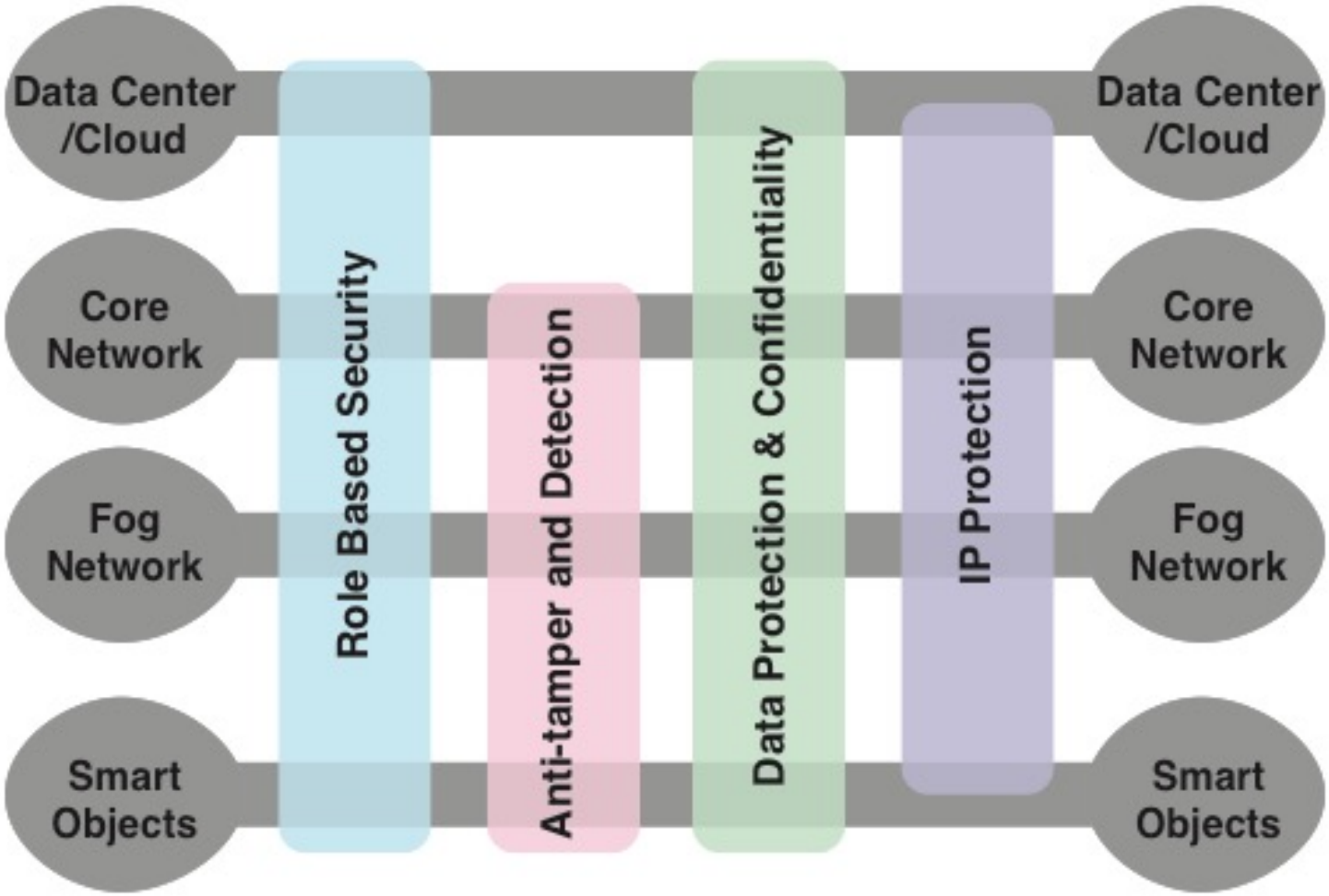


Figure 13.12 IoT Security Environment

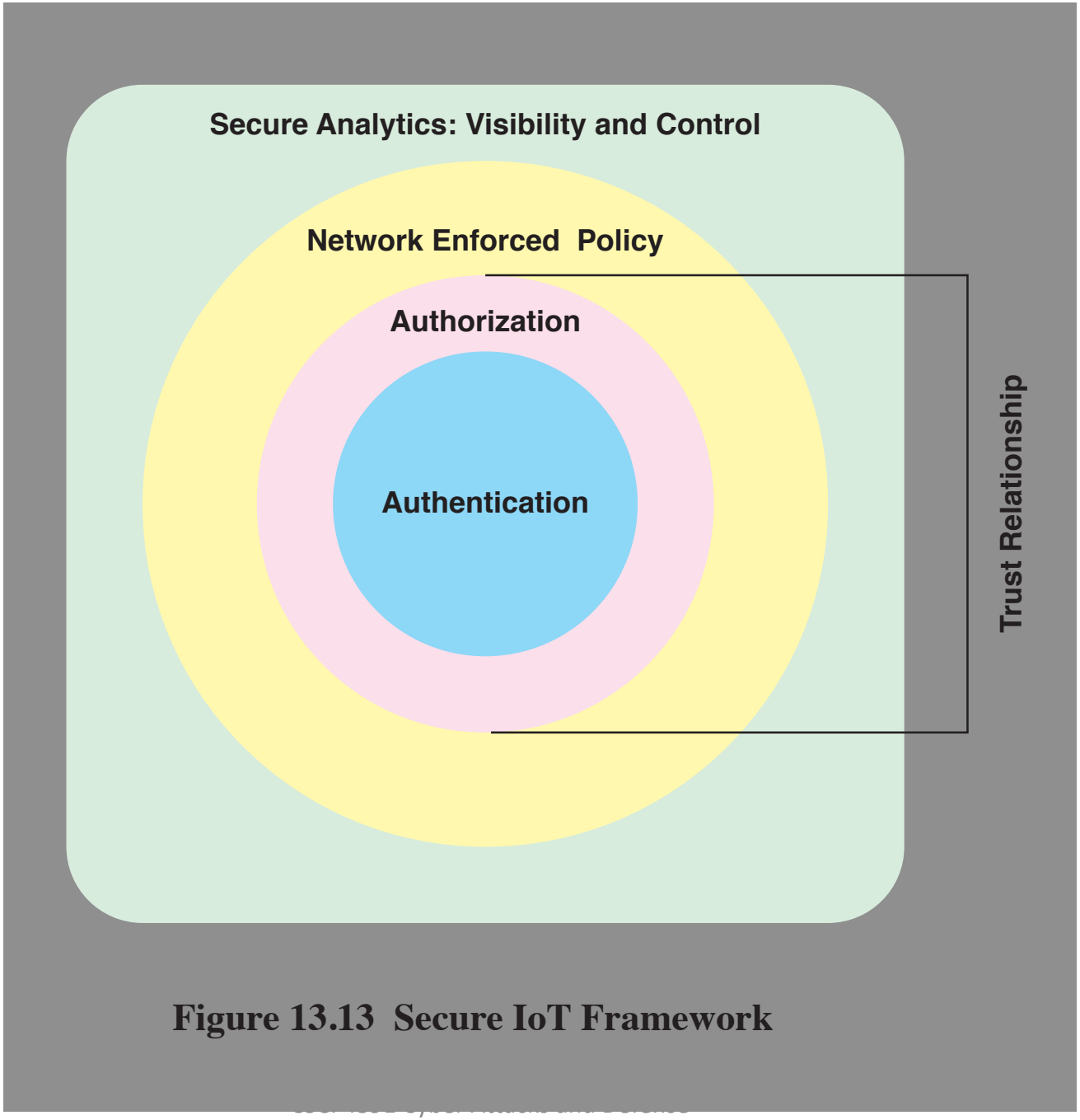


Figure 13.13 Secure IoT Framework

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 (Cont.)

- MiniSec is designed to meet the following requirements:
  - Data authentication
  - Confidentiality
  - Replay protection
  - Freshness
  - Low energy overhead
  - Resilient to lost messages