

A large, glowing blue padlock is the central focus of the image. It is set against a dark, textured background that features faint, glowing binary code (0s and 1s) scattered across it. The padlock itself has a bright blue outline and a glowing blue body, with a dark blue keyhole. The overall aesthetic is high-tech and digital.

Cloud, IoT and Wireless Security

Chapter 13 & 24

Dr Naveed Khan

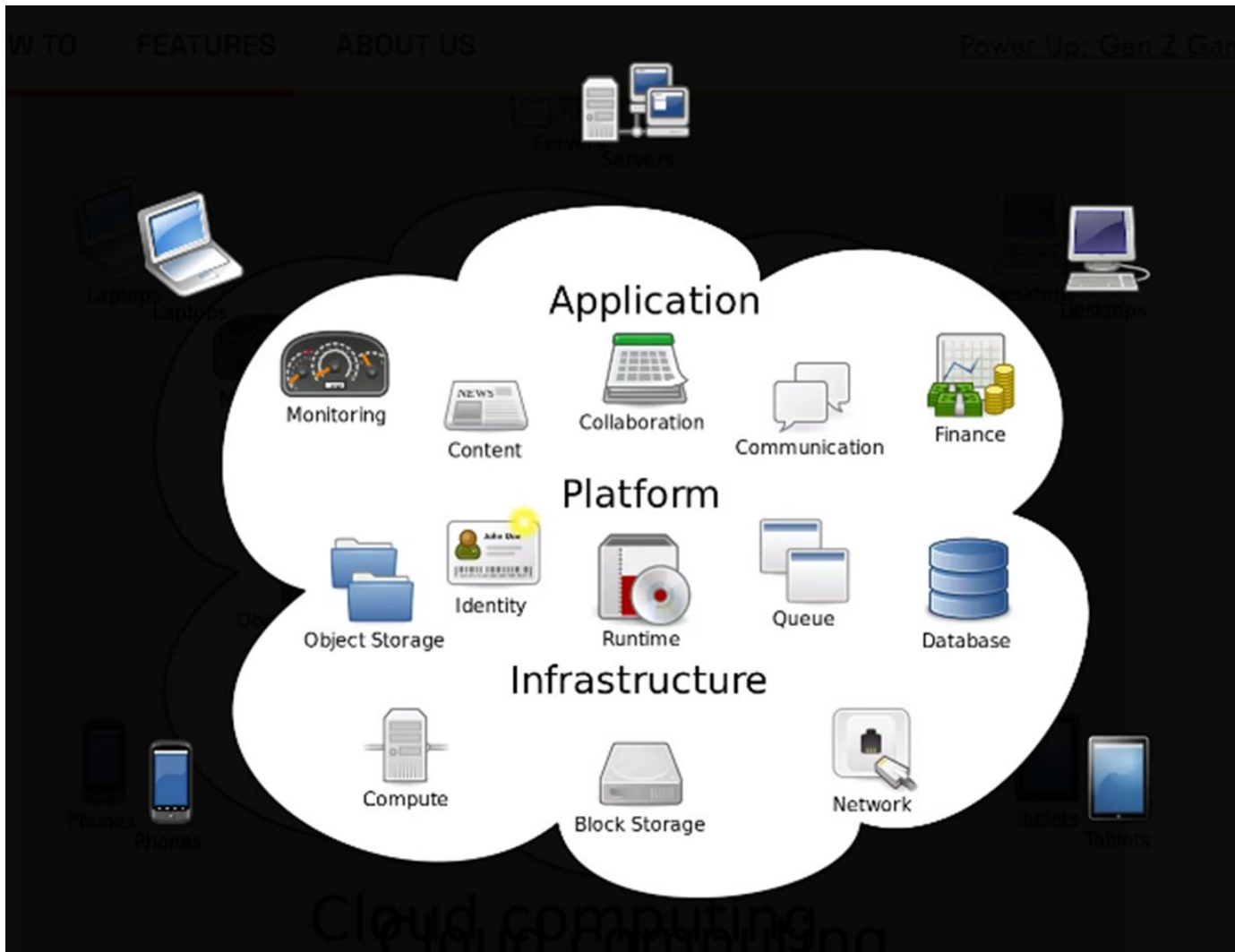
n.khan@ulster.ac.uk

COM398

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.”



Cloud Computing Architecture

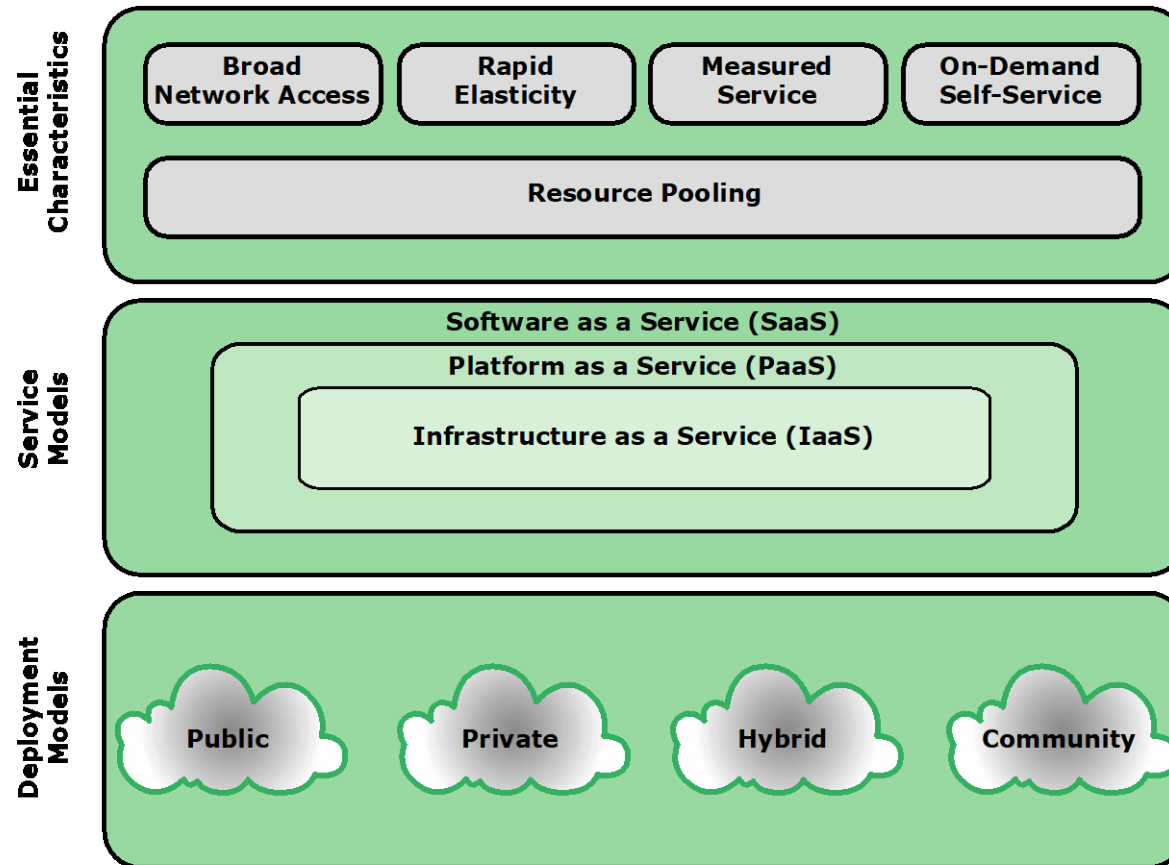
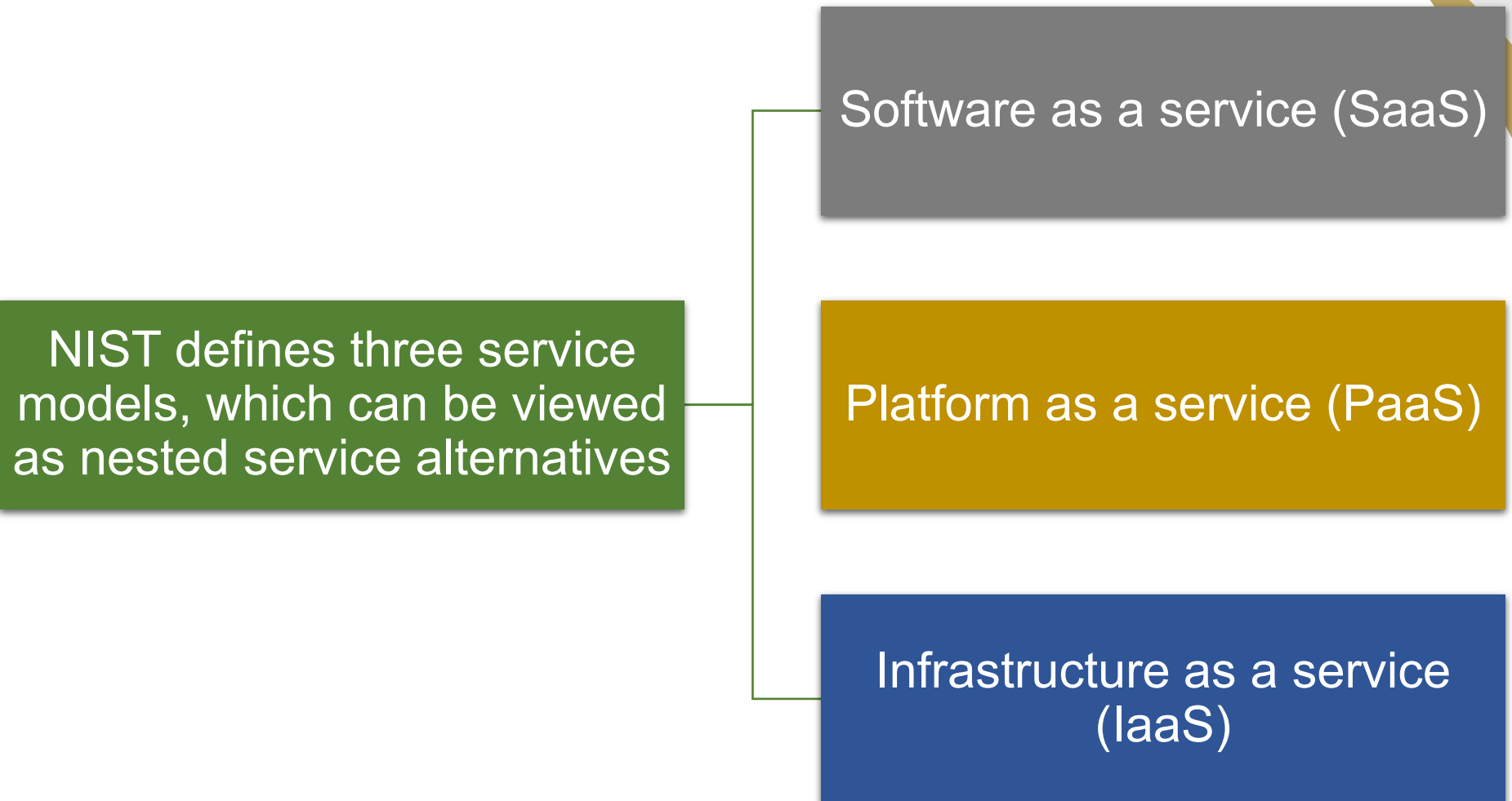


Figure 13.1 Cloud Computing Elements

Cloud Service Models



Infrastructure as a Service (IaaS)

- Cloud Providers offer virtualized computing resources over the internet.
- Resources typically include virtual machine (VMs), Storage, and networking components.
- Users of IaaS have more control over the Infrastructure compared to other service models.
- Provision and manage VMs , install software , and configure networking settings.
 - Examples
 - Amazon Web Service (AWS)
 - Microsoft Windows Azure
 - Google Cloud Compute Engine (GCE).

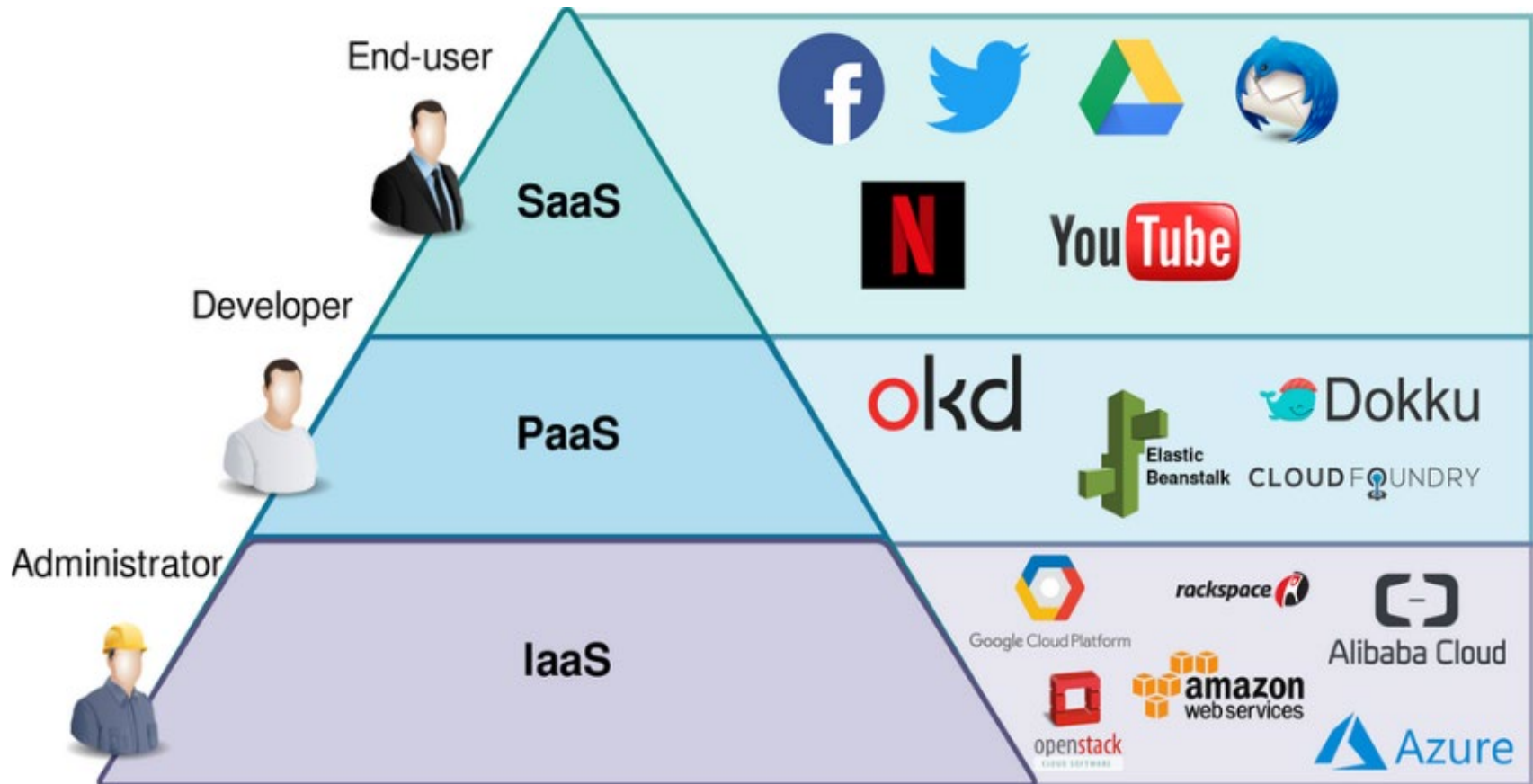
Platform as a Service (PaaS)

- Provides a platform and environment for developers to build, deploy, and manage applications without worrying about the underlying infrastructure.
- Developers can focus on coding and application logic.
- In a PaaS environment, the cloud provider manages the infrastructure, including the operating system, runtime environment, and development tools.
- Examples of PaaS offerings include
 - Google Colab
 - Dokku
 - Cloud Foundry
 - Heroku.

Software as a Service (SaaS)

- SaaS is a cloud service model where cloud providers deliver software applications over the internet on a subscription basis.
- Users access these applications through web browsers without the need for installation or maintenance.
- With SaaS, users have little to no control over the underlying infrastructure or application code. They simply use the software as it's provided by the service provider.
- Examples of SaaS applications include
 - Gmail,
 - Facebook,
 - Twitter,
 - YouTube.

Cloud Services Types Examples



Cloud Deployment Models

Public cloud

Community cloud

The four most prominent deployment models for cloud computing are:

Private cloud

Hybrid cloud


Public Cloud

- In a public cloud deployment, Cloud resources and services are owned and operated by a third-party cloud service provider, and they are made available to the general public or a wide range of customers.
- These resources are hosted in data centers owned and managed by the cloud provider.
- Public cloud services are typically accessible over the internet, and users pay for the resources they consume on a pay-as-you-go basis.
- The major advantage of the public cloud is cost
- The principal concern is security
- Examples of Public Cloud Providers are
 - Amazon Web Service (AWS),
 - Microsoft Azure
 - Google Cloud Platform

Private Cloud



A private cloud is implemented within the internal IT environment of the organization



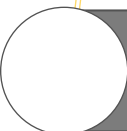
The organization may choose to manage the cloud in house or contract the management function to a third party



The cloud servers and storage devices may exist on premise or off premise



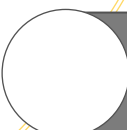
Private clouds offer greater control, security, and customization options compared to public clouds.



Examples of services delivered through the private cloud include database on demand, email on demand, and storage on demand

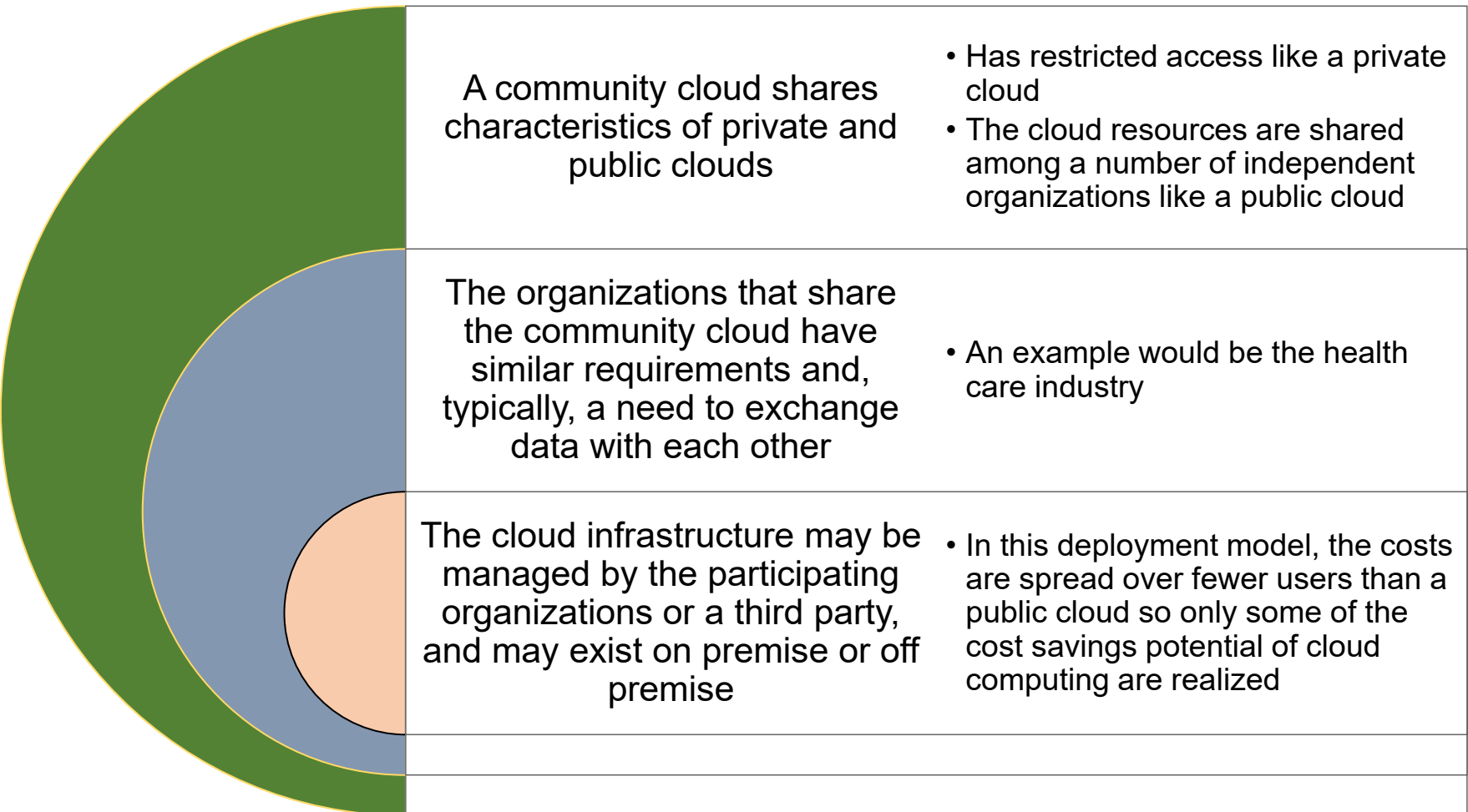


A key motivation for opting for a private cloud is security



Other benefits include easy resource sharing and rapid deployment to organizational entities

Community Cloud



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

Security Issues for Cloud Computing

- Security is a major consideration when augmenting or replacing on-premises systems with cloud services
- Cloud security is a critical consideration for organizations that use cloud services.
- Cloud computing offers numerous benefits, it also introduces unique security challenges and risks.
- Common cloud security issues and risks
 - Abuse and nefarious use of cloud computing
 - Insecure interfaces and APIs
 - Malicious insiders
 - Shared technology issues
 - Data loss or leakage
 - Account or service hijacking

Risks and Countermeasures

- **The Cloud Security Alliance lists the following as the top cloud-specific security threats:**
- Abuse and nefarious use of cloud computing (Phishing, DDoS)
- 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 (Weak auth, Lack of encryption & validation)
- 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

- **Malicious insiders (Data theft, Service disruption)**
- Countermeasures include:
 - Implement strict access control policies and the principle of least privilege. Limit user access to only the resources and data necessary for their job roles.
 - 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 (Shared Memory, Shared Storage)**
- Countermeasures include:
 - Implement security best practices for installation/configuration
 - Monitor the environment for unauthorized changes/activity
 - Promote strong authentication and access control for administrative access and operations

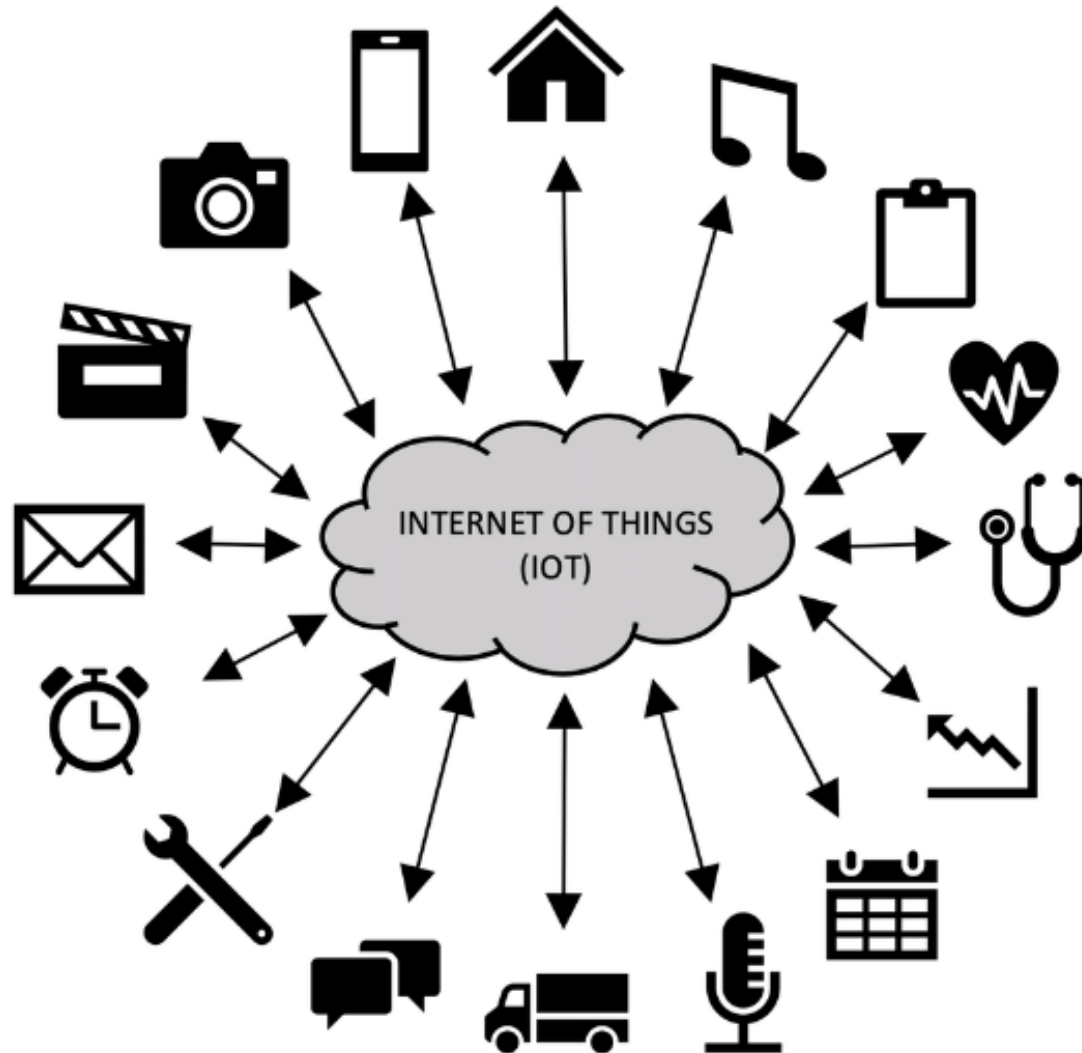
Risks and Countermeasures

- **Data loss or leakage** (deleted Accidentally, Unauthorized Access)
- 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** (Brute force attacks, Compromised credentials)
- 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

The Internet of Things (IoT)

- IoT is a network of interconnected physical devices or smart devices ranging from appliances to tiny sensors.
- These devices can transfer data to one another without human intervention.
- IoT devices are not limited to computers or machinery.
- The Internet of Things can include anything with a sensor that is assigned a unique identifier (UID).
- The primary goal of the IoT is to create self-reporting devices that can communicate with each other (and users) in real time.

The Internet of Things (IoT)



The Internet of Things (IoT) - Examples

- **Wearable Health Devices:** Fitness trackers and smartwatches can monitor a person's heart rate, sleep patterns, and activity levels, providing valuable health data.
- **Smart Home Security Systems:** IoT-enabled security cameras, motion detectors, and doorbell cameras allow homeowners to monitor their properties remotely and receive alerts in real time..
- **Industrial IoT (IIoT):** Manufacturing plants use IoT sensors and devices to monitor equipment, predict maintenance needs, and improve operational efficiency.
- **Smart Lighting:** IoT-connected light bulbs can be controlled via smartphones and programmed to adjust brightness and color temperature based on user preferences.

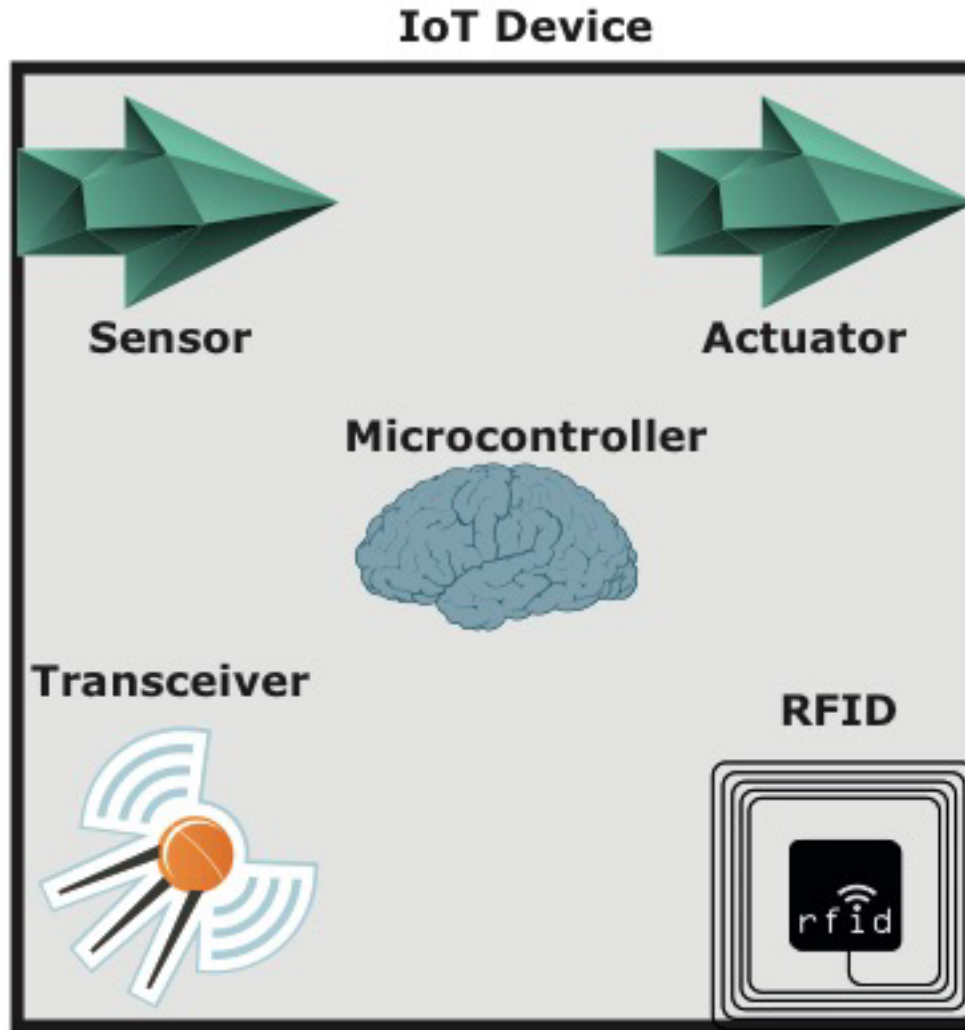
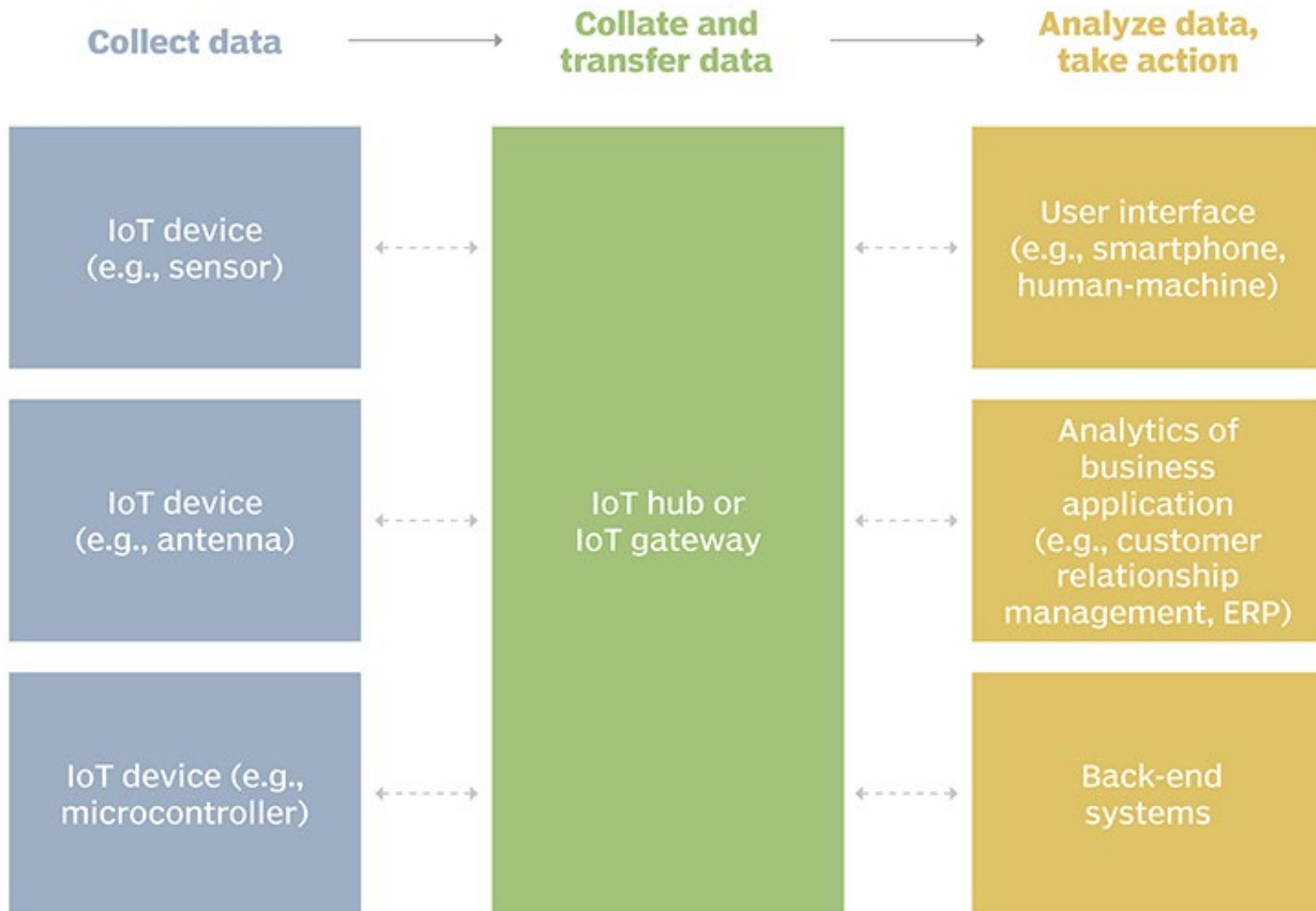


Figure 13.8 IoT Components

Example of an IoT system ?



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

IoT Security and Privacy Requirements

- **Communication security**
 - unauthorized access to the content of data can be prohibited, integrity of data can be guaranteed and privacy-related content of data can be protected during data transmission
- **Data management security**
 - unauthorized access to the content of data can be prohibited, integrity of data can be guaranteed, and privacy-related content of data can be protected when storing or processing data in IoT.
- **Service provision security**
 - unauthorized access to service and fraudulent service provision can be prohibited and privacy information related to IoT users can be protected

IoT Security and Privacy Requirements

- **Integration of security policies and techniques**
 - Ability to integrate different security policies and techniques
 - To ensure a consistent security control over the variety of devices and user networks in IoT.
- **Mutual authentication and authorization**
 - Mutual authentication and authorization between the device (or the IoT user) and IoT is required to be performed according to predefined security policies
- **Security audit**
 - Any data access or attempt to access IoT applications are required to be fully transparent, traceable and reproducible according to appropriate regulation and laws.

Wireless Security

- Key factors contributing to higher security risk of wireless networks compared to wired networks include:
- Channel
 - Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks
 - Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols
- Mobility
 - Wireless devices are far more portable and mobile, thus resulting in a number of risks
- Resources
 - Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware
- Accessibility
 - Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations, thus greatly increasing their vulnerability to physical attacks

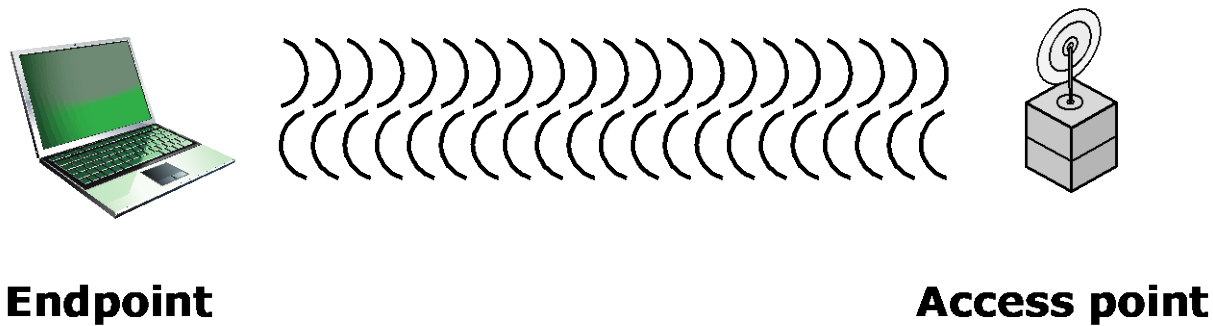


Figure 24.1 Wireless Networking Components

Wireless Network Threats

**Accidental
association**

**Malicious
association**

**Ad hoc
networks**

**Nontraditional
networks**

**Identity theft
(MAC
spoofing)**

**Man-in-the
middle
attacks**

**Denial of
service (DoS)**

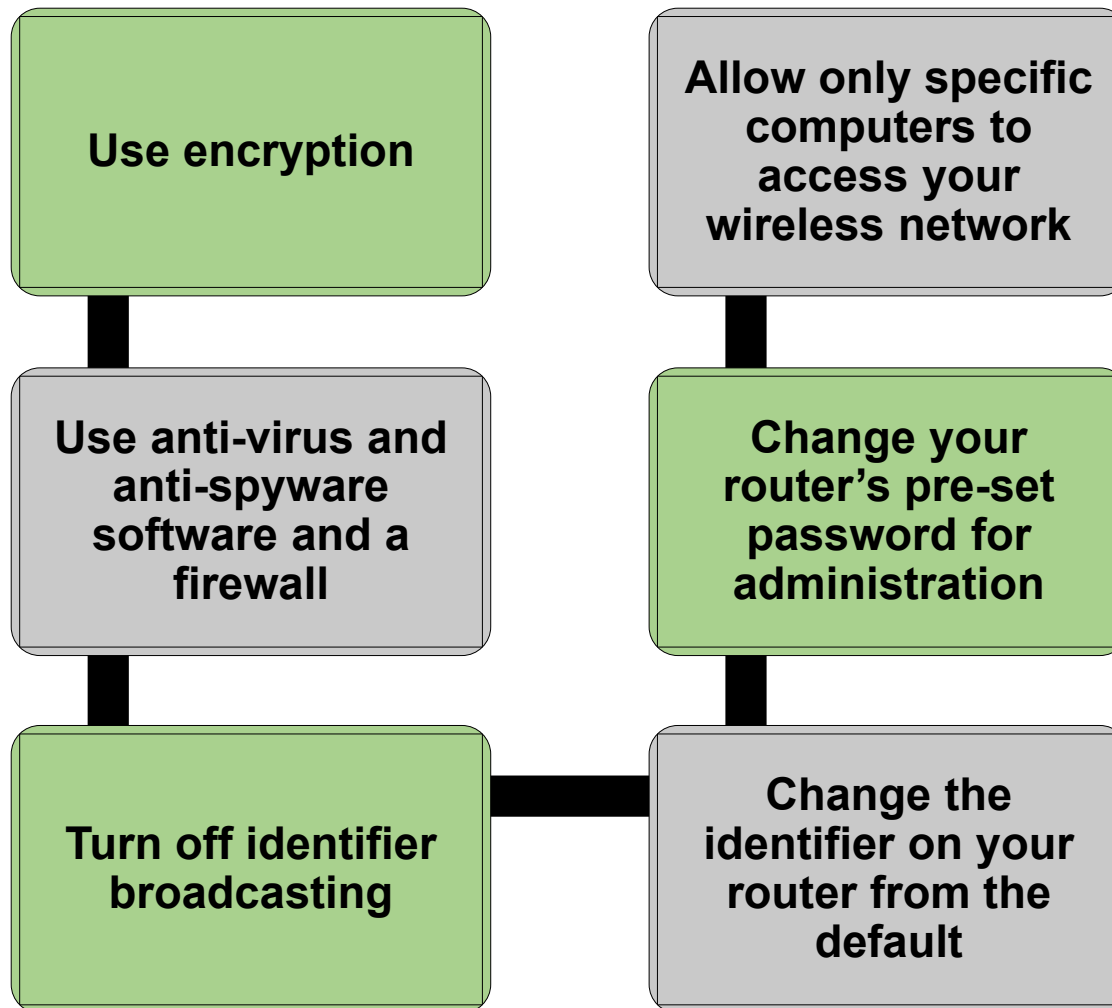
Securing Wireless Transmissions

- Principal threats are eavesdropping, altering or inserting messages, and disruption
- Countermeasures for eavesdropping:
 - Signal-hiding techniques
 - Encryption
- The use of encryption and authentication protocols is the standard method of countering attempts to alter or insert transmissions

Securing Wireless Networks

- The main threat involving wireless access points is unauthorized access to the network
- Principal approach for preventing such access is the IEEE 802.1X standard for port-based network access control
- The standard provides an authentication mechanism for devices wishing to attach to a LAN or wireless network
- Use of 802.1X can prevent rogue access points and other unauthorized devices from becoming insecure backdoors

Wireless Network Security Techniques



Thanks!