INTRODUCTION TO IoT SECURITY

Mr. Rajasekar V.R.
Department of Information Technology
Sur College of Applied Sciences
Ministry of Higher Education
Sultanate of Oman

CONTENT

12.1 The IoT Era Begins
12.2 Components of IoT-Enabled Things
12.3 IoT Reference model
12.4 IoT Security
12.5 IoT Security & Privacy Req. defined by ITU-T
12.6 An IoT Security Framework
12.7 IoT Security Challenges
12.8 Internet of Things - Liability
12.9 IoT security tools

12.1 The IoT Era Begins

- The future Internet will involve large numbers of objects that use standard communications architectures to provide services to end users.
- It is envisioned that tens of billions of such devices will be interconnected in a few years.
- This will provide new interactions between the physical world and computing, digital content, analysis, applications, and services.
- This resulting networking paradigm is being called the Internet of Things (IoT).

- This will provide unprecedented opportunities for users, manufacturers, and service providers in a wide variety of sectors.
- Areas that will benefit from IoT data collection, analysis, and automation capabilities include health and fitness, healthcare, home monitoring and automation, energy savings and smart grid, farming, transportation, environmental monitoring, inventory and product management, security, surveillance, education, and many others.

- According to ITU-T Y.2060: Internet of Things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

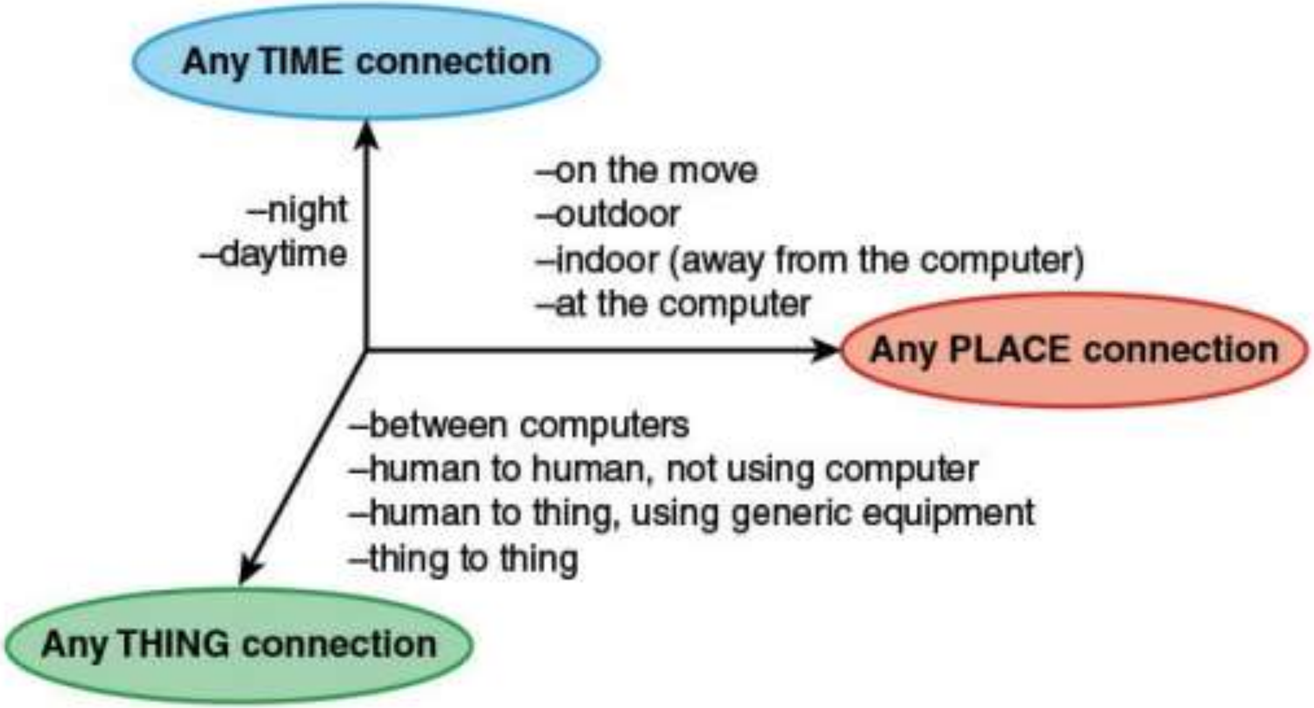
- Thing: With regard to the IoT, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

- Device: With regard to the IoT, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage, and data processing.

- **Physical objects + Controllers, Sensors, Actuators + Internet = IoT.**

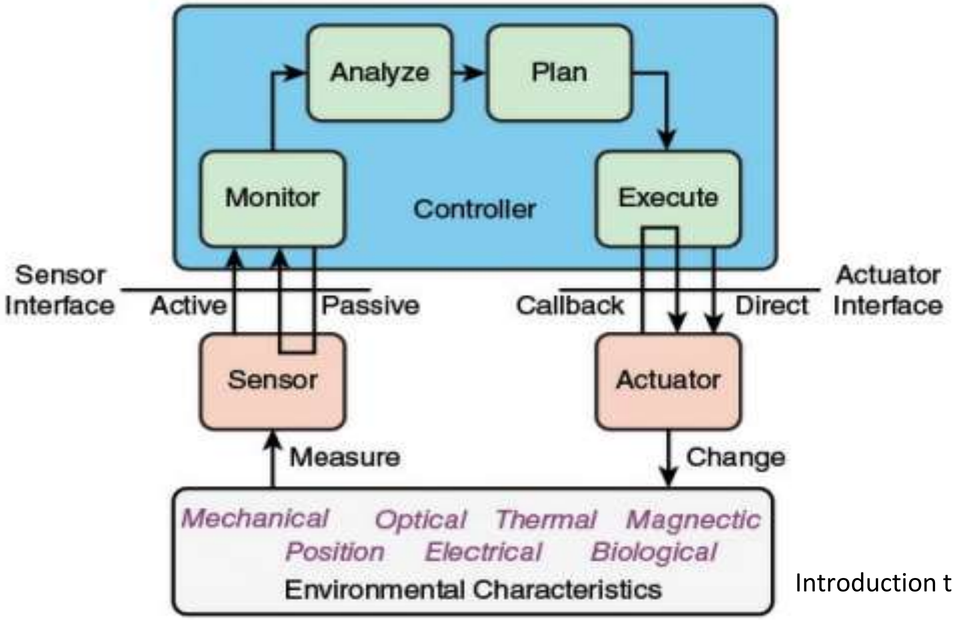
- An instance of the IoT consists of a collection of physical objects, each of which:
  - Contains a microcontroller that provides intelligence
  - Contains a sensor that measures some physical parameter/actuator that acts on some physical parameter.
  - Provides a means of communicating via the Internet or some other network.

- IoT is characterized as adding the dimension “Any THING communication” to the information and communication technologies which already provide “any TIME” and “any PLACE” communication as show in the figure.



12.2 Components of IoT-Enabled Things

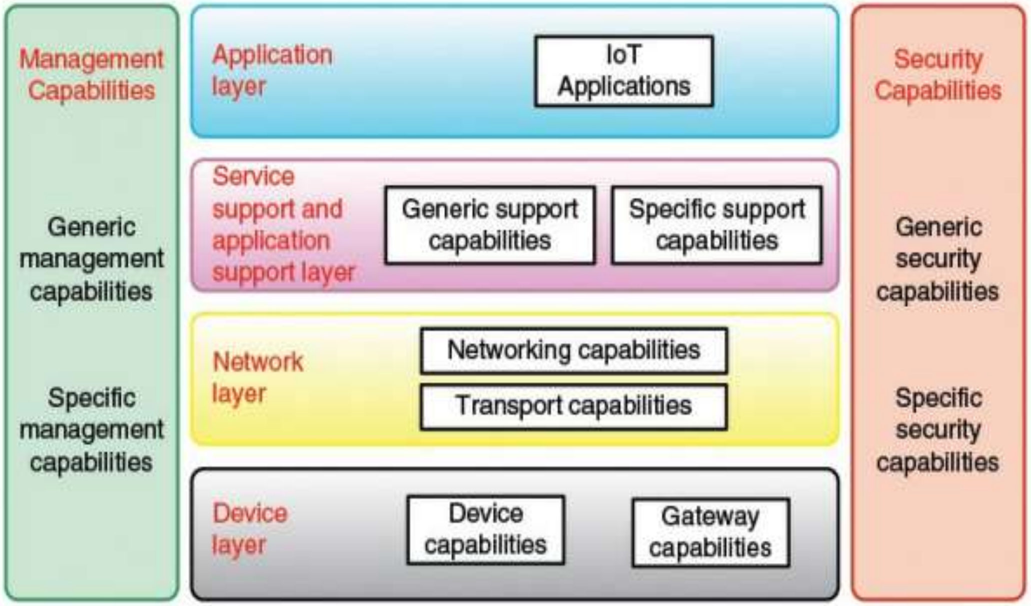
- The key ingredients of an IoT-enabled thing are sensors, actuators, a microcontroller, a means of communication (transceiver), and a means of identification.
- A means of communication is an essential ingredient; otherwise, the device cannot participate in a network.
- Nearly all IoT-enabled things have some sort of computing capability, no matter how rudimentary and a device may have one or more of the other ingredients.
- Following diagram shows the interfaces for sensors and actuators.



12.3 IoT Reference model

- ITU-T IoT reference model, consists of four layers as well as management capabilities and security capabilities that apply across layers.

- In terms of communications functionality, the device layer includes, roughly, the OSI physical and data link layers.



Management Capabilities

Generic management capabilities

Specific management capabilities

Application layer

IoT Applications

Service support and application support layer

Generic support capabilities

Specific support capabilities

Network layer

Networking capabilities

Transport capabilities

Device layer

Device capabilities

Gateway capabilities

Security Capabilities

Generic security capabilities

Specific security capabilities

- The security capabilities layer includes generic security capabilities that are independent of applications.

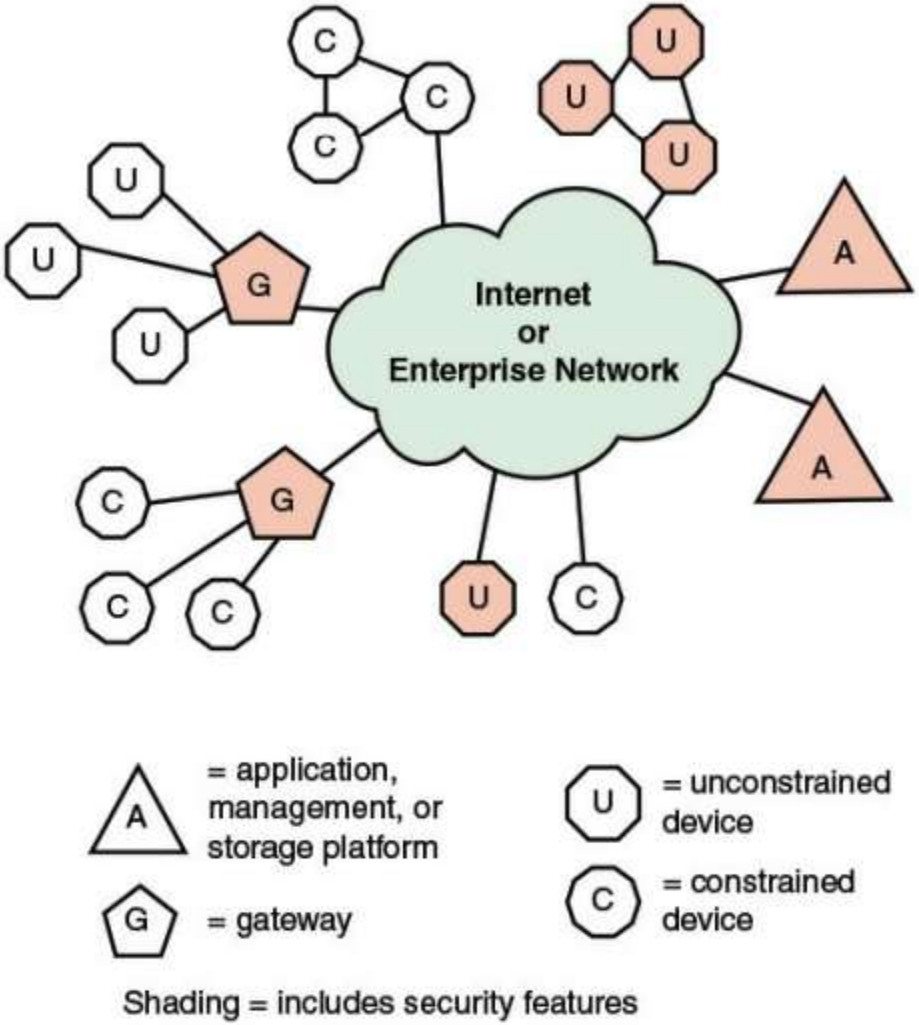
  Application layer: Authorization, authentication, application data confidentiality and integrity protection, privacy protection, security audit, and antivirus.

  Network layer: Authorization, authentication, user data and signaling data confidentiality, and signaling integrity protection

  Device layer: Authentication, authorization, device integrity validation, access control, data confidentiality, and integrity protection.

12.4 IoT Security

- IoT is perhaps the most complex and undeveloped area of network security.
- Below figure shows the main elements of interest for IoT security.
- At the center of the network are the application platforms, data storage servers, and network and security management systems.
- These central systems gather data from sensors, send control signals to actuators, and are responsible for managing the IoT devices and their communication networks.
- At the edge of the network are IoT-enabled devices, some of which are quite simple constrained devices and some of which are more intelligent unconstrained devices.
- As well, gateways may perform protocol conversion and other networking service on behalf of IoT devices.
- The shading in Figure - indicates the systems that support at least some of the functions like TLS and IPsec.
- Unconstrained devices may or may not implement some security capability.
- Constrained devices generally have limited or no security features.
- Gateway devices can provide secure communication between the gateway and the devices at the center, such as application platforms and management platforms.


Internet or Enterprise Network
U
G
C
A
= application, management, or storage platform
= gateway
= unconstrained device
= constrained device
Shading = includes security features

12.5 IoT Security and Privacy Requirements Defined by ITU-T

- ITU-T Recommendation Y.2066, Common Requirements of the Internet of Things, June 2014, includes a list of security requirements for the IoT. The requirements are as follows:

- **Communication security:** Secure, trusted, and privacy-protected communication capability is required, so that 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 or transfer in IoT.

- **Data management security:** Secure, trusted, and privacy-protected data management capability is required, so that 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:** Secure, trusted, and privacy-protected service provision capability is required, so that unauthorized access to service and fraudulent service provision can be prohibited and privacy information related to IoT users can be protected.

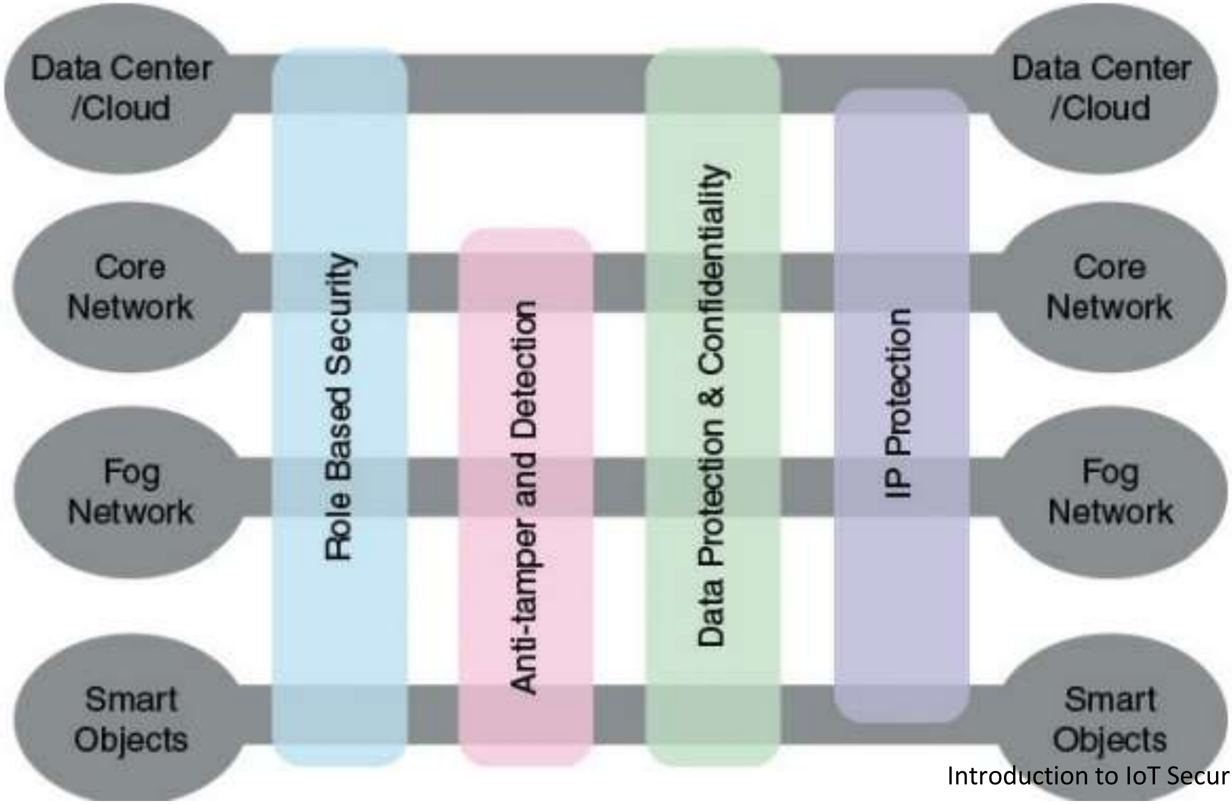
- **Integration of security policies and techniques:** The ability to integrate different security policies and techniques is required, so as to ensure a consistent security control over the variety of devices and user networks in IoT.

- **Mutual authentication and authorization:** Before a device (or an IoT user) can access the IoT, 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:** Security audit is required to be supported in IoT. Any data access or attempt to access IoT applications are required to be fully transparent, traceable and reproducible according to appropriate regulation and laws. In particular, IoT is required to support security audit for data transmission, storage, processing, and application access.

12.6 An IoT Security Framework

- Below figure, illustrates the security environment related to the logical structure of an IoT.
- The IoT model is a simplified version of the World Forum IoT Reference Model.
- It consists of the following levels:



12.6.1 Smart objects/embedded systems:

- Consists of sensors, actuators, and other embedded systems at the edge of the network.
- The devices may not be in a physically secure environment.
- Availability is certainly an issue. Need to be concerned about the authenticity and integrity of the data generated by sensors.
- Protecting actuators and other smart devices from unauthorized use, privacy and protection from eavesdropping may also be requirements.

12.6.2 Fog/edge network:

- This level is concerned with the wired and wireless interconnection of IoT devices.
- A key issue of concern is the wide variety of network technologies and protocols used by the various IoT devices and the need to develop and enforce a uniform security policy.

12.6.3 Core network:

- Provides data paths between network center platforms and the IoT devices.
- The security issues here are those confronted in traditional core networks.
- However, the vast number of endpoints to interact with and manage creates a substantial security burden.

12.6.4 Data center/cloud:

- This level contains the application, data storage, and network management platforms.
- IoT does not introduce any new security issues at this level, other than the necessity of dealing with huge numbers of individual endpoints.

Within this four-level architecture, the four general security capabilities that span multiple levels are:

1. Role-based security:

- RBAC systems assign access rights to roles instead of individual users.
- In turn, users are assigned to different roles, either statically or dynamically, according to their responsibilities.
- RBAC enjoys widespread commercial use in cloud and enterprise security and is a well-understood tool that can be used to manage access to IoT devices and the data they generate.

2. Antitamper and detection:

- This function is particularly important at the device and fog network levels but also extends to the core network level.
- All of these levels may involve components that are physically outside the area of the enterprise that is protected by physical security measures.

3. Data protection and confidentiality: These functions extend to all level of the architecture.

4. Internet protocol protection: Protection of data in motion from eavesdropping and snooping is essential between all levels.

12.7 IoT Security Challenges

- Beyond costs and the ubiquity of devices, other security issues plague IoT:

12.7.1 Unpredictable Behavior:

- The sheer volume of deployed devices and their long list of enabling technologies means their behavior in the field can be unpredictable.
- A specific system may be well designed and within administration control, but there are no guarantees about how it will interact with others.

12.7.2 Device Similarity:

- IoT devices are fairly uniform.
- They utilize the same connection technology and components.
- If one system or device suffers from a vulnerability, many more have the same issue.

12.7.3 Problematic Deployment:

- One of the main goals of IoT remains to place advanced networks and analytics where they previously could not go.
- Unfortunately, this creates the problem of physically securing the devices in these strange or easily accessed places.

12.7.4 Long Device Life and Expired Support:

- One of the benefits of IoT devices is longevity, however, that long life also means they may outlive their device support.
- Compare this to traditional systems which typically have support and upgrades long after many have stopped using them.
- Orphaned devices and abandon-ware lack the same security hardening of other systems due to the evolution of technology over time.

12.7.5 No Upgrade Support:

- Many IoT devices, like many mobile and small devices, are not designed to allow upgrades or any modifications.
- Others offer inconvenient upgrades, which many owners ignore, or fail to notice.

12.7.6 Poor or No Transparency:

- Many IoT devices fail to provide transparency with regard to their functionality.
- Users cannot observe or access their processes, and are left to assume how devices behave.
- They have no control over unwanted functions or data collection; furthermore, when a manufacturer updates the device, it may bring more unwanted functions.

12.7.7 No Alerts:

- Another goal of IoT remains to provide its incredible functionality without being obtrusive.
- This introduces the problem of user awareness.
- Users do not monitor the devices or know when something goes wrong.
- Security breaches can persist over long periods without detection.

12.8 Internet of Things - Liability

- The security flaws of IoT and its ability to perform certain tasks open the door to any associated liability.
- The three main areas of concern are device malfunction, attacks, and data theft.
- These issues can result in a wide variety of damages.

12.8.1 Device Malfunction

- IoT introduces a deeper level of automation which can have control over critical systems, and systems impacting life and property.
- When these systems fail or malfunction, they can cause substantial damage; for example, if an IoT furnace control system experiences a glitch, it may fail in an unoccupied home and cause frozen pipes and water damage.
- This forces organizations to create measures against it.

12.8.2 Data Theft

- Data, IoT's strength and weakness, proves irresistible to many.
- These individuals have a number of reasons for their interest − the value of personal data to marketing/advertising, identity theft, framing individuals for crimes, stalking, and a bizarre sense of satisfaction.
- Measures used to fight attacks are also effective in managing this threat.

12.8.3 Cyber Attacks

- IoT devices expose an entire network and anything directly impacted to the risk of attacks.
- Though those connections deliver powerful integration and productivity, they also create the perfect opportunity for mayhem like a hacked stove or fire safety sprinkler system.
- The best measures against this address the most vulnerable points, and provide custom protections such as monitoring and access privileges.
- Some of the most effective measures against attacks prove simple:
- **Built-in Security** − Individuals and organizations should seek hardened devices, meaning those with security integrated in the hardware and firmware.
- **Encryption** − This must be implemented by the manufacturer and through user systems.
- **Risk Analysis** − Organizations and individuals must analyze possible threats in designing their systems or choosing them.
- **Authorization** − Devices, whenever possible, must be subject to privilege policies and access methods.

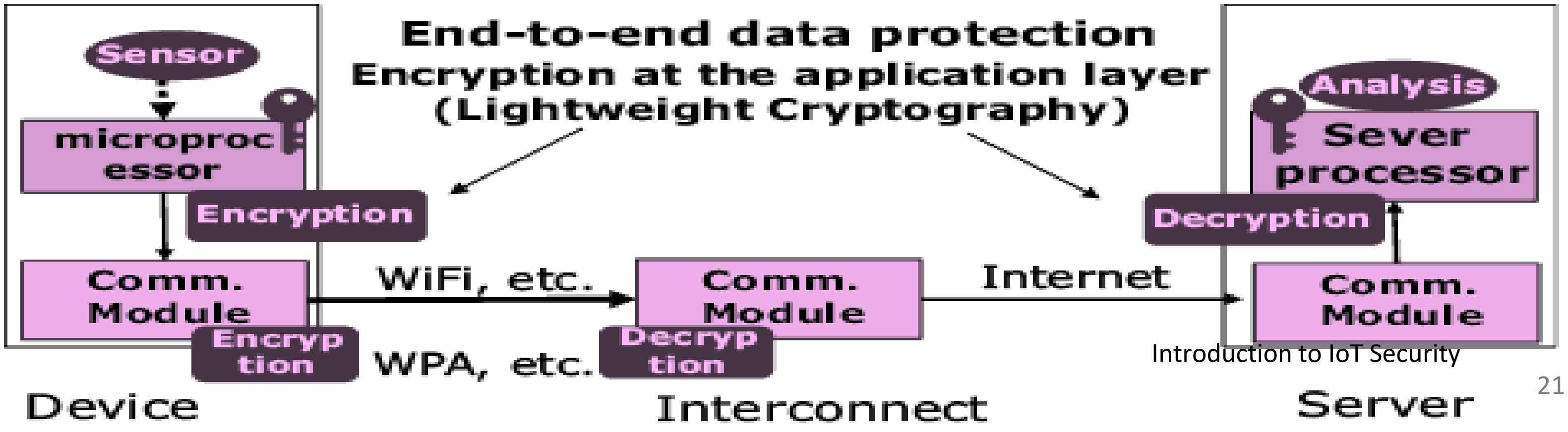
12.9 IoT security tools

The common security tools that are in use are:

1. Encryption
2. Password Protection
3. Hardware Security Modules
4. Two-factor authentication
5. Secure elements
6. Data erasure
7. PKI Certifications
8. Biometrics
9. Hardware Crypto processor
10. Blockchain

12.9.1 Encryption

- "Lightweight Cryptography (LWC)" - a cryptographic algorithm or protocol tailored for implementation in constrained environments including RFID tags, sensors, contactless smart cards, health-care devices and so on.
- The lightweight primitives are superior to conventional cryptographic ones, which are currently used in the Internet security protocols, e.g. IPsec, TLS.
- Lightweight cryptography also delivers adequate security.
- Lightweight cryptography does not always exploit the security-efficiency trade-offs.

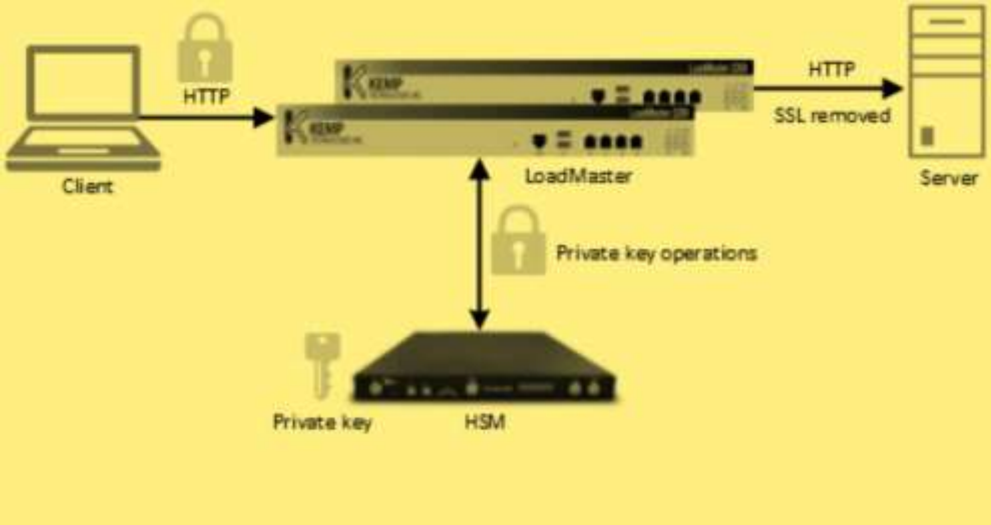


12.9.2 Password Protection

- Password-based authentication starts to look less attractive as a security solution for IoT devices, for two reasons:
- Passwords don't work well on dumb devices. They lack the power to process or store passwords.
- Passwords are a poor means of automated authentication. Entering a password generally requires a human to do something, and that's hard to automate. As a result, passwords aren't good for securing automated exchanges of information.

2.9.3 Hardware Security Modules

- A **hardware security module** (**HSM**) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.
- These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server.
- The functions of an HSM are:
- onboard secure cryptographic key generation
- onboard secure cryptographic key storage and management
- use of cryptographic and sensitive data material
- offloading application servers for complete asymmetric and symmetric cryptography.



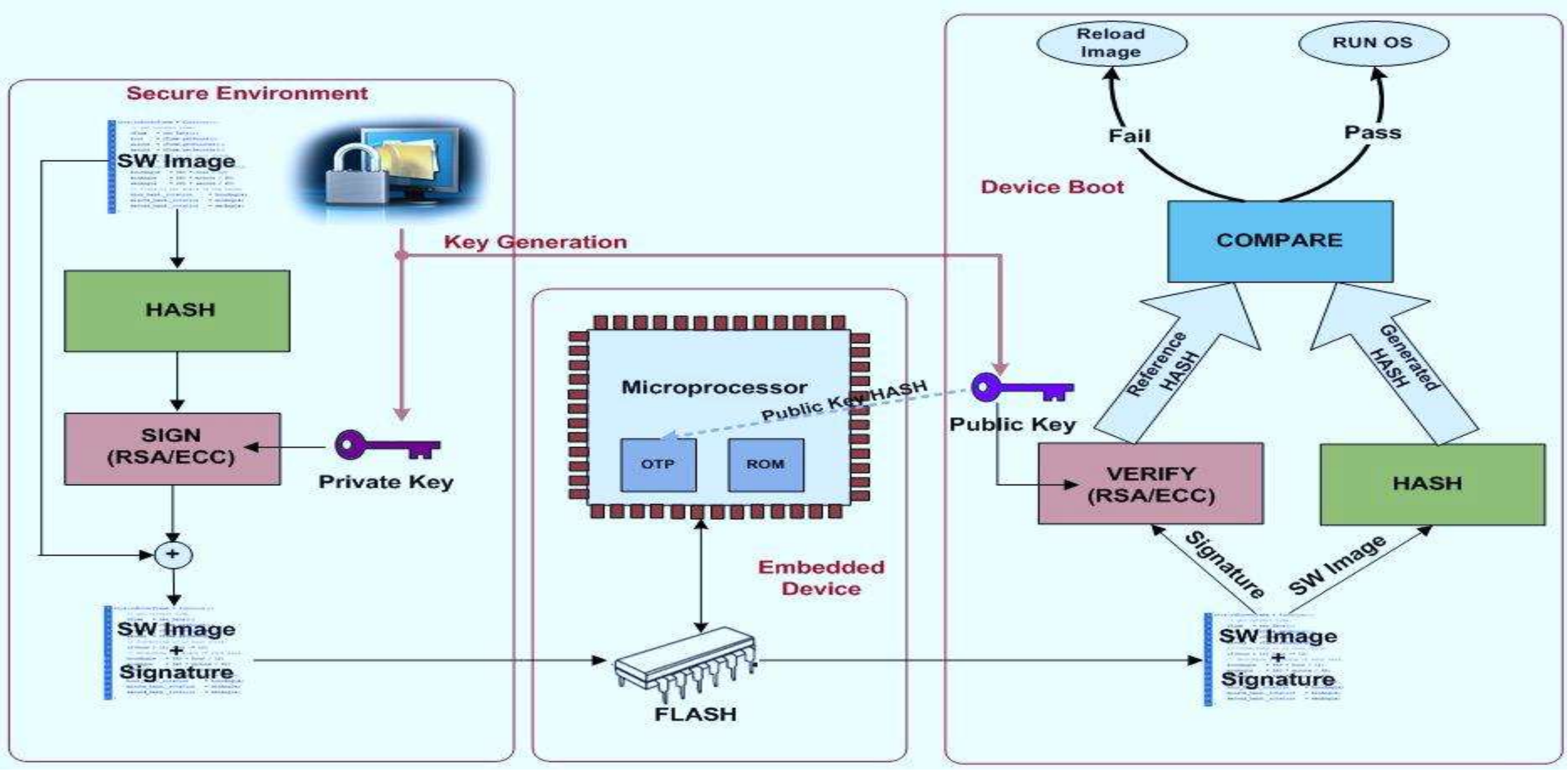
2.9.4 Two-factor authentication

- Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are.
- 2FA can be contrasted with single-factor authentication(SFA), a security process in which the user provides only one factor- typically a password.
- Two-factor authentication provides an additional layer of security and makes it harder for attackers to gain access.
- Two-factor authentication has long been used to control access to sensitive systems and data.
- 2FA to prevent their users' data from being accessed by attackers.

TWO-FACTOR AUTHENTICATION
Pick any two: Something you KNOW, something you HAVE, something you ARE
Username

2.9.5 Embedded Security software blocks

- The embedded security software block is a tamper-proof chip available in different sizes and designs, embedded in any mobile device.
- It ensures the data is stored in a safe place and information is given to only authorized applications and people.
- It is like a personal ID for the end-user and for the device itself.



2.9.6 Secure elements

- The Secure Element is a tamper resistant hardware component embedded in IoT and industrial connected equipment and machines to deliver smart card level digital security and device lifecycle management.
- The Secure Element serves as the foundation of trust in advanced end-to-end security architecture that protects data integrity and defends against cyber-attacks.
- Secure elements ensure that data is stored in a safe place and that access is granted only to authorized applications and people.
- It also enables over-the-air management of security credentials, software updates and evolving security capabilities across the lifecycle of solutions.

2.9.7 Data erasure

- Data erasure (sometimes referred to as data clearing or data wiping) is a software-based method of overwriting the data that aims to completely destroy all electronic data residing on a hard disk drive or other digital media by using zeros and ones to overwrite data onto all sectors of the device.
- By overwriting the data on the storage device, the data is rendered unrecoverable and achieves data sanitization.
- Ideally, software designed for data erasure should:
- Allow for selection of a specific standard, based on unique needs, and
- Verify the overwriting methodology has been successful and removed data across the entire device.

2.9.8 PKI Certifications

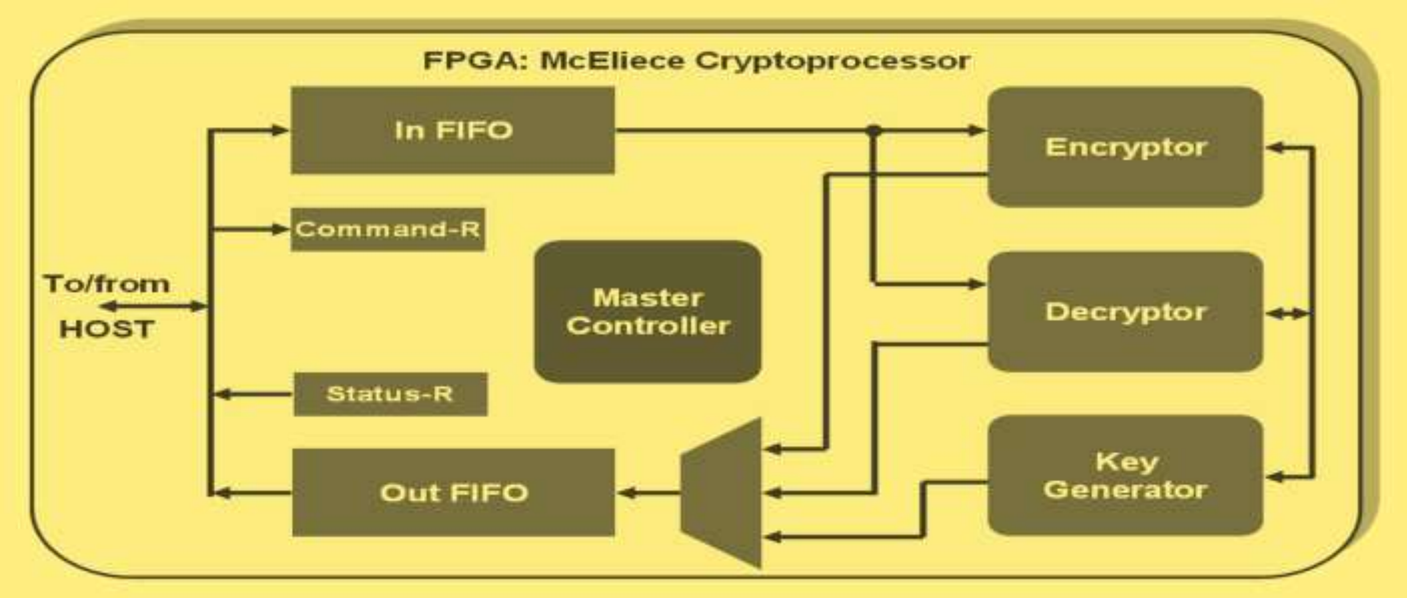
- A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
- The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.
- It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

2.9.9 Biometrics

- Biometric authentication is the process of comparing data for the person's characteristics to that person's biometric "template" in order to determine resemblance.
- The reference model is first store in a database or a secure portable element like a smart card.
- The data stored is then compared to the person's biometric data to be authenticated.
- Here it is the person's identity which is being verified.

2.9.10 Hardware Crypto processor

- A secure cryptoprocessor is a dedicated computer on a chip or microprocessor for carrying out cryptographic operations, embedded in a packaging with multiple physical security measures, which give it a degree of tamper resistance.
- Unlike cryptographic processors that output decrypted data onto a bus in a secure environment, a secure cryptoprocessor does not output decrypted data or decrypted program instructions in an environment where security cannot always be maintained.
- The purpose of a secure cryptoprocessor is to act as the keystone of a security subsystem, eliminating the need to protect the rest of the subsystem with physical security measures



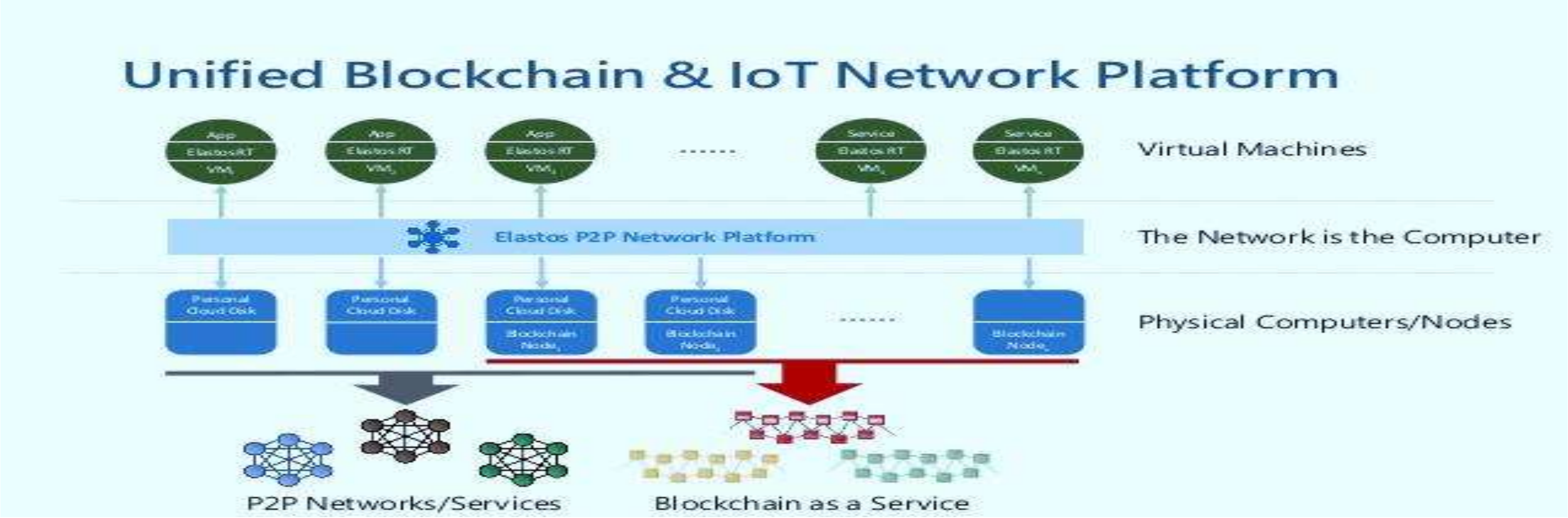
2.9.11 Blockchain

- Blockchain is a database that maintains a continuously growing set of data records.
- It is distributed in nature, meaning that there is no master computer holding the entire chain.
- Rather, the participating nodes have a copy of the chain.
- It’s also ever-growing — data records are only added to the chain.
- A blockchain consists of two types of elements:

1. Transactions are the actions created by the participants in the system.

2. Blocks record these transactions and make sure they are in the correct sequence and have not been tampered with. Blocks also record a time stamp when the transactions were added.

- Blockchain technology offers a way of recording transactions or any digital interaction in a way that is designed to be secure, transparent, highly resistant to outages, auditable, and efficient; as such, it carries the possibility of disrupting industries and enabling new business models.
- By merging Blockchain with IoT it is easier to implement confidentiality and integrity.
- This allows the connected devices to respond to fabrication and modification attacks and enhances the trust between the parties in communication."


Unified Blockchain & IoT Network Platform
App
Elastos RT
VM_1
App
Elastos RT
VM_2
App
Elastos RT
VM_3
......
Service
Elastos RT
VM_x
Service
Elastos RT
VM_n
Virtual Machines
Elastos P2P Network Platform
The Network is the Computer
Personal Cloud Disk
Personal Cloud Disk
Personal Cloud Disk
Blockchain $Node_1$
Personal Cloud Disk
Blockchain $Node_2$
......
Blockchain $Node_n$
Physical Computers/Nodes
P2P Networks/Services
Blockchain as a Service