IOT Security

The basic security goals in IoT

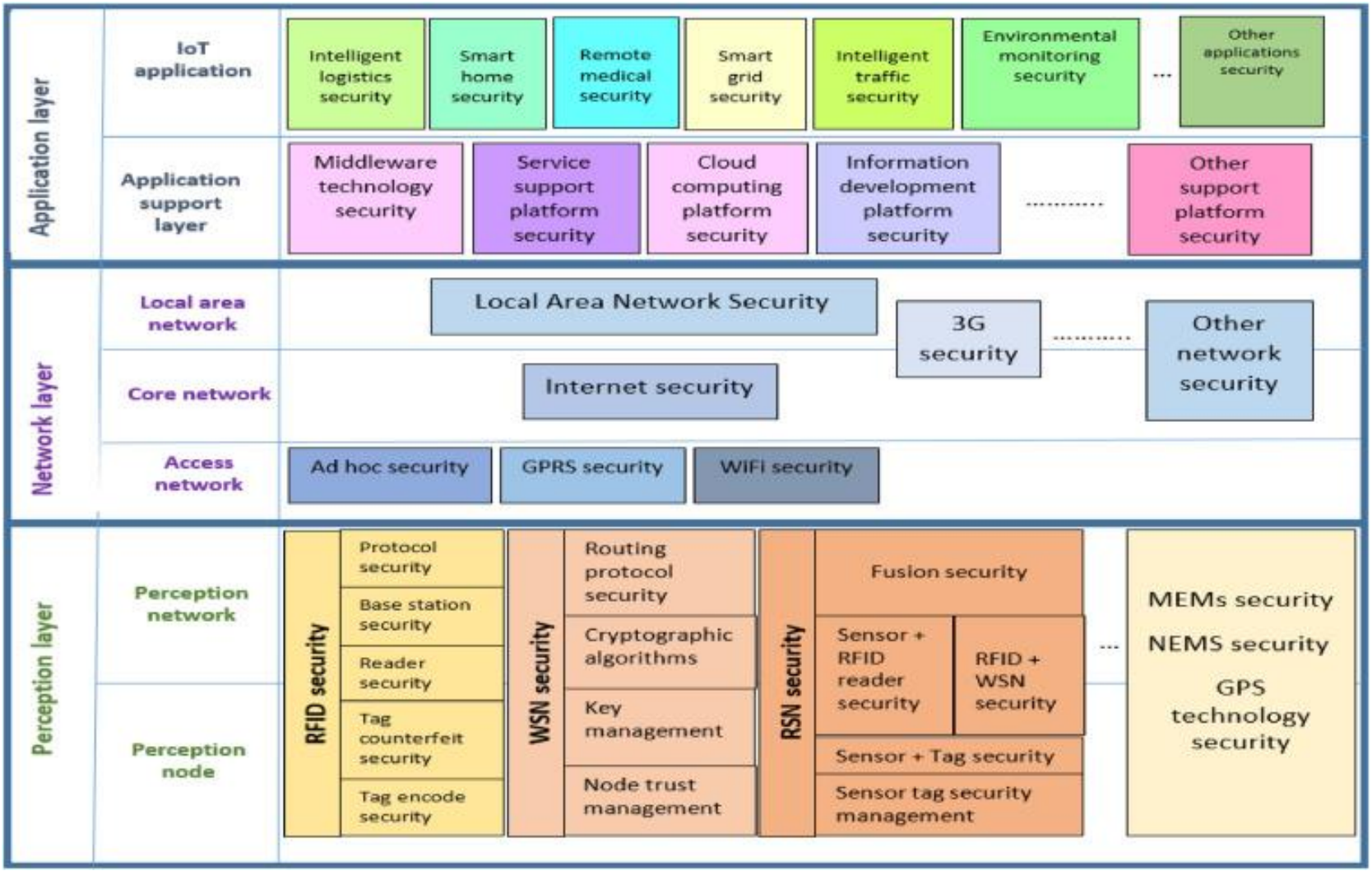
- 1. Confidentiality: The message is only disclosed to authorized entities, user, nodes, devices, and services; the confidentiality is about the controlling for devices, message access. The private data, keys, and security credentials must be well protected from unauthorized entities.
- 2. Integrity, the original message is not tampered with: In IoT systems, different applications may have various integrity requirements, such as e-healthcare system may have more restricted data integrity than the general smart cities applications.
- 3. Authentication and authorization: The connectivity of the devices aggravates the problem of authentication because of the access control and the nature of wireless communication in IoT systems.
- 4. Availability: The system keeps serving its purpose and stays uninterruptedly available for legitimate entities. The IoT systems are required to be robust to provide services for accessing anytime.
- 5. Accountability: To improve the robustness of services in IoT environment, accountability of IoT systems is necessary.

Attack techniques in IoT environment

- 1. **Physical attacks**, which means attack tampers with physical components. In some case, the IoT devices might be deployed in outdoor environment, which brings risks to IoT systems.
- 2. **Eavesdropping** is the process of overhearing an ongoing communication, which is as well preliminary for launching the next two attacks. Since in IoT environment, many IoT end-nodes are interconnected wirelessly and everyone is able to access the medium. Confidentiality is a typical counter-measurement against eavesdroppers. However, if the keying material is not exchanged in a secure manner, the eavesdropper could be able to compromise the confidentiality. Therefore, secure key change algorithms, such as DH (Diffie-Hellman), are used in the practical scenario.
- 3. **Impersonation** is when a malicious entity pretends to be another, mostly legitimate, entity, for instance will be replaying a genuine message, in order to bypass the aforementioned security goals. A special form of this attack is the man-in-the-middle (MITM) attack.

- 4**. MITM** attack takes place when a malicious entity is on the network path of two genuine entities. Hence, it is capable of delaying, modifying, or dropping messages. MITM attack is interesting within the context of public-key cryptography (PKC). Then the malicious entity does not attempt to break the keys of involved parties, but rather to become the falsely trusted MITM. The malicious user achieves this by replacing the exchanged keys with its own. This way each of the parties establishes a secure channel with the malicious user, who gains access to messages in plain text.
- 5. **DoS** (Denial of Service) attack targets the availability of a system that offers services. This is achieved by exhaustingly consuming resources at the victim so that the offered services become unavailable to legitimate entities. A common way to launch this attack is to trigger expensive operations at the victim that consume resources, such as computational power, memory, bandwidth, or energy. This attack is critical for constrained devices, where existing resources are already scarce.
- 6. Access attacks that involve attacks unauthorized entities gain access to IoT systems or devices.
- 7. Other attacks, such as firmware attack as “bad USB,” attacks on privacy, RAM attacks, channel side attack, ransomware, etc.

Security in IOT Architecture



Vulnerability in The Layers

	RFID attacks	WSN attacks
Layer	Possible attacks	Possible attacks
Physical/Link	Jammers, replay attacks, Sybil, selective forwarding, synchronization attack.	Passive interference, active jamming of temporarily disabling the device, Sybil, destruction of RFID readers, replay attacks
Network/Transport	Sinkhole, unfairness, false routing, hello and session flooding, eavesdropping.	**Tag attacks:** Cloning, spoofing **Reader attacks:** Impersonation, eavesdropping **Network protocol attacks**
Application Layer	Injection, buffer overflows	Injection, buffer overflows, unaithorized tag reading, tag modification
Multi-layer attack	Side channel attack, replay attacks, traffic analysis, crypto attack	Side channel attack, replay attacks, traffic analysis, crypto attack

Hardware Level Security

- IoT devices typically use a Real Time Operating System (RTOS)which includes
  - a microkernel,
  - hardware abstraction layer,
  - communication drivers,
  - capabilities such as process isolation, secure boots, and application sandbox.
- The concerns regarding the IoT hardware are
  - authentication capabilities,
  - end-to-end traffic encryption,
  - secure boot-loading process,
  - the enforcement of digital signatures during firmware updates,
  - transparent transactions.

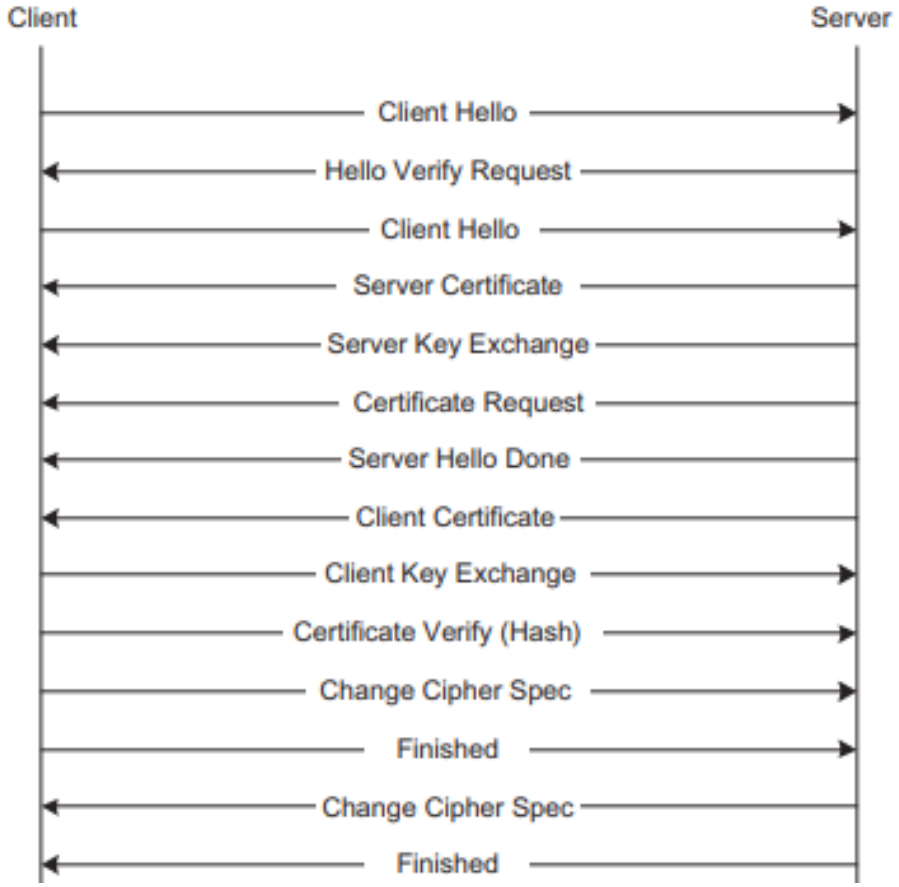
TransportLayer

- Lack of Transport encryption concerns an insecure communication link between
  - device and the Cloud,
  - device and gateway,
  - device and mobile applications,
  - one device and another device, and
  - communication between the gateway and the Cloud.

Network Layer And Application Layer

- Authentication and Authorization are the most popular security method to achieve secure communication in the network layer.
- Insecure web and cloud interfaces are vulnerabilities that may be an attack vector in an IoT system at the application layer.
  - Thus, the cloud gateways have to be equipped with security controls to restrict bad actors from modifying configurations.
  - Applying biometrics and multi-level authentication for access control might be a good solution at the application layer.

Hand shake based Authentication Verification



Current Security Issues and Ways to Resolve

Layer	Security challenges	Mitigation
Perception	Detection of the abnormal sensor node	fault detection algorithm, decentralized intrusion detection system
	The choice cryptography algorithms and key management mechanism to be used	public key encryption due to the large scale network
		slot reservation protocol
	Data and sender anonymity	Access control, mitigation of resource depletion attacks
	Device vulnerabilities	
Network	Enabling IPSec communication with IPv6 nodes	Research in the suitability of IPv6 and IPSec for secure communication.
Application	Configurable embedded computer systems.	Biometric verification

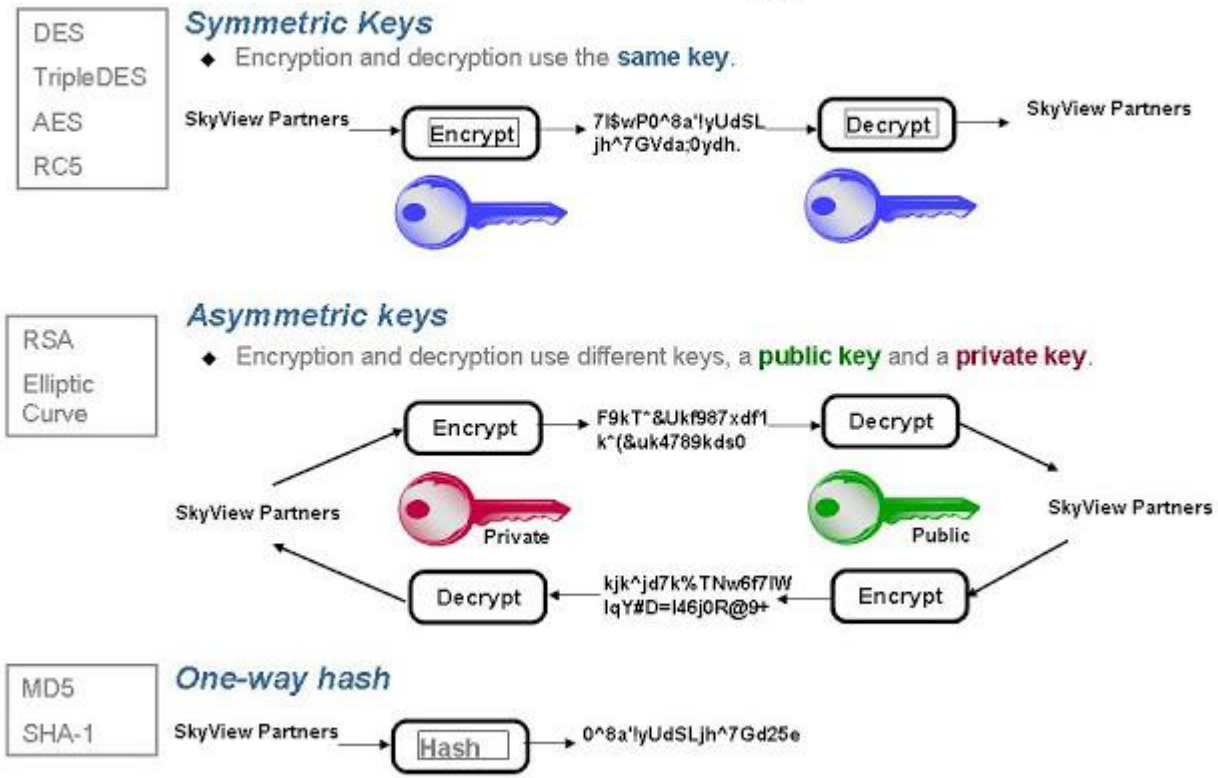
Authentication Methods

- Public-key encryption, in which one is capable of encrypting a message with the public key of an entity, where only the entity with the corresponding private key is capable of decrypting the cipher text.
- Digital signatures in which a cipher text generated with the private key can be decrypted by anyone who has the public key. This verification proves that the sender had access to the private key and therefore is likely to be the person associated with the public key.

Authentication

- Authentication is the process of identifying users and devices in a network and granting access to authorized persons and non-manipulated devices.
- Authentication is one way to mitigate attacks to the IoT systems such as
  - the reply attack,
  - the Man-in-the-Middle attack,
  - the impersonation attack
  - the Sybil attack.
  - Authentication is currently still the most popular method (60%) to grant access to the user at the application layer and also give access to the device in the IoT network.

Types of Encryption



- **Symmetric encryption** uses a single **key** that needs to be shared among the people who need to receive the message
- **asymmetrical encryption** uses a pair of public **key** and a private **key** to encrypt and decrypt messages when communicating. ...**Asymmetric encryption** takes relatively more time than the **symmetric encryption**.

Weaknesses of the current solutions for IoT

- 1)Stolen verifier attack and many logged-in users with the same login ID attack.
- 2)Denial-of-service attack and node capture attack.
- 3)Replay attack and forgery attack.
- 4)Stolen smart-card and sensor-node impersonation.
- 5)Gateway node bypassing and sensor-node key impersonation.
- 6)Off-line password guessing attack, off-line identity guessing attack, smart card theft attack, user impersonation attack, sensor node impersonation attack.

Crytographic Algorithms for Authentication

Asymmetric algorithm	Key size	Code length	Possible attack
RSA	1024	900	Modules attack
ECC	160	8838	Timing attack

Symmetric algorithm	Code length	Structure	Number of rounds	Key size	Block size	Possible attacks
AES	2606	SPN	10	128	128	Man-in-the-middle attacks
HEIGHT	5672	GFS	32	128	64	Saturation attack
TEA	1140	Feistel	32	128	64	Related key attack
PRESENT	936	SPN	32	80	64	Differential attack
RC5	Not fixed	ARX	20	16	32	Differential attack

Trust Based Authentication

- Trust is the degree of belief about the future behavior of other entities, which is based on the ones the past experience with and observation of the others actions.

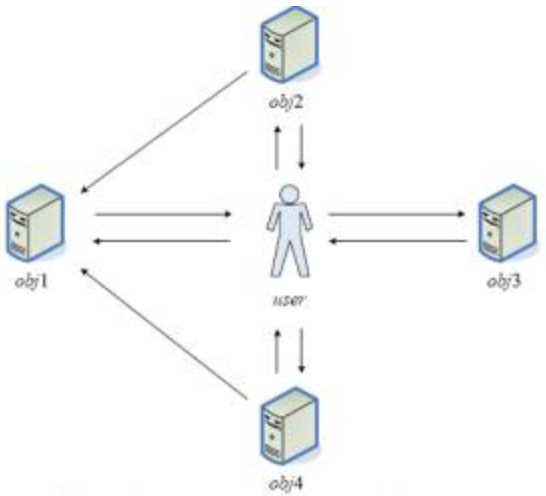


Figure 1. Structure of authentication mechanism

Relationship based on trust

- Trust and reputation have been recently suggested as an effective security mechanism for open environments such as the Internet and considerable research has been done on modeling and managing trust and reputation
- Trust management systems are designed to deal with selfish behaviors or internal attacks and not to assist cryptographic measures.
- Our solution evaluates the trust level related to the presence of security threats among nodes, and adapt consequently cryptographic measures. T

BlockChains

- Block chains are used to incorporate trust based authentication methods
- Advantage
  - Useful for heterogeneous devices and systems
  - serves to create secure virtual zones (*bubbles*) where things can identify and trust each other
- Disadvantages
  - Computing resource availability

Thanks