Securing Internet of things Infrastructure Standard and Techniques

Paper Author : Zubair A. Baig

Name: Farooq Abdullah
M.Sc Programming and Networks
University of Oslo.

Security internet of Things Standards and Techniques

Overview:

Internet of things Infrastructure

- Electronic Devices interconnected through the Internet to provide effective Service to the End Users.
- It handles sensitive information Such as Patient Health care Record ,Position of the logistic Vehicle, temperature readings form the Sensor Nodes.
- Protection of Such sensitive Information is very important.
- The paper Gives the analysis of standards and techniques for protecting communication channels in IOT.

Introduction

- The devices constituting IOT architecture are tiny for example RFID tags, wireless Sensors.
- The advances in the Communication and processing capabilities of small devices make it possible to communicate with them overlong distances.
- Interaction of these small IOT devices require efficient and secure communication with the System.
- The provision of security and privacy depends on the IOT Device Used.

Security for Wireless Sensor Network

- Wireless Devices called sensor nodes transfer the sensor data to high performance base station.
- Such Networks will serve several Application like Environmental Monitoring, health Monitoring, early Warning applications.
- Sensor nodes are capable of providing Advanced Encryption Standard AES based encryption and decryption of communication channel between node and its gateway.

Security in Wireless Sensor Network

- On of the most common threat to security of such networks is reading the data secretly when it is transmitted from sensor node to base station.
- Privacy is achieved by Secret Shared key based mechanism. Where sensor node-base station pairs will possesses the secret shared key.
- The data is encrypted with symmetric key encryption (AES) and decrypted at the receivers end using the same shared key.

Wireless Security

- Alternative way to secure the communication channel is to use public key Cryptography.
- Need more processing power result in quick consumption of battery of wireless sensor nodes.
- The integrity of Sensor data is also very important so that It cannot be tempered and lead to the misleading results.
- Affective approach to solve this problem is the use of Message authentication Code (MAC).

Wireless Security

- MAC is the hash of message with the secret key shared between sender and receiver. Hash function used is SHA1 or MD5
- A message appended with current time and or a fresh nonce can help to prevent reply attacks
- Jamming attacks can b avoided by frequency hopping and random time slots technique

RFID Tag Security

- It is the primary concern to provide Security to RFID tags is the limitation of computation resources in these device.
- Encryption of RFID tag Data is due to limited resources in the devices.
- The security concerns can be solved using public private key pairs or through symmetric keys. However limit on the key length due to limitation of resource in RFID tags exposes such devices to Brute force attacks and Dictionary attacks.

WI-Fi Security

- WI-Fi is helpful in establishing wireless local area networks on large scale and provide users connection to the internet.
- By default WI-FI operates in encryption free mode so unless the application service provider such as online banking server does not provide secure communication channel. It is not recommended to communicate passwords and other sensitive information on WIFI.
- WIFI uses wifi protection Access (WPA or WPA2) for to provide security to communication channel.

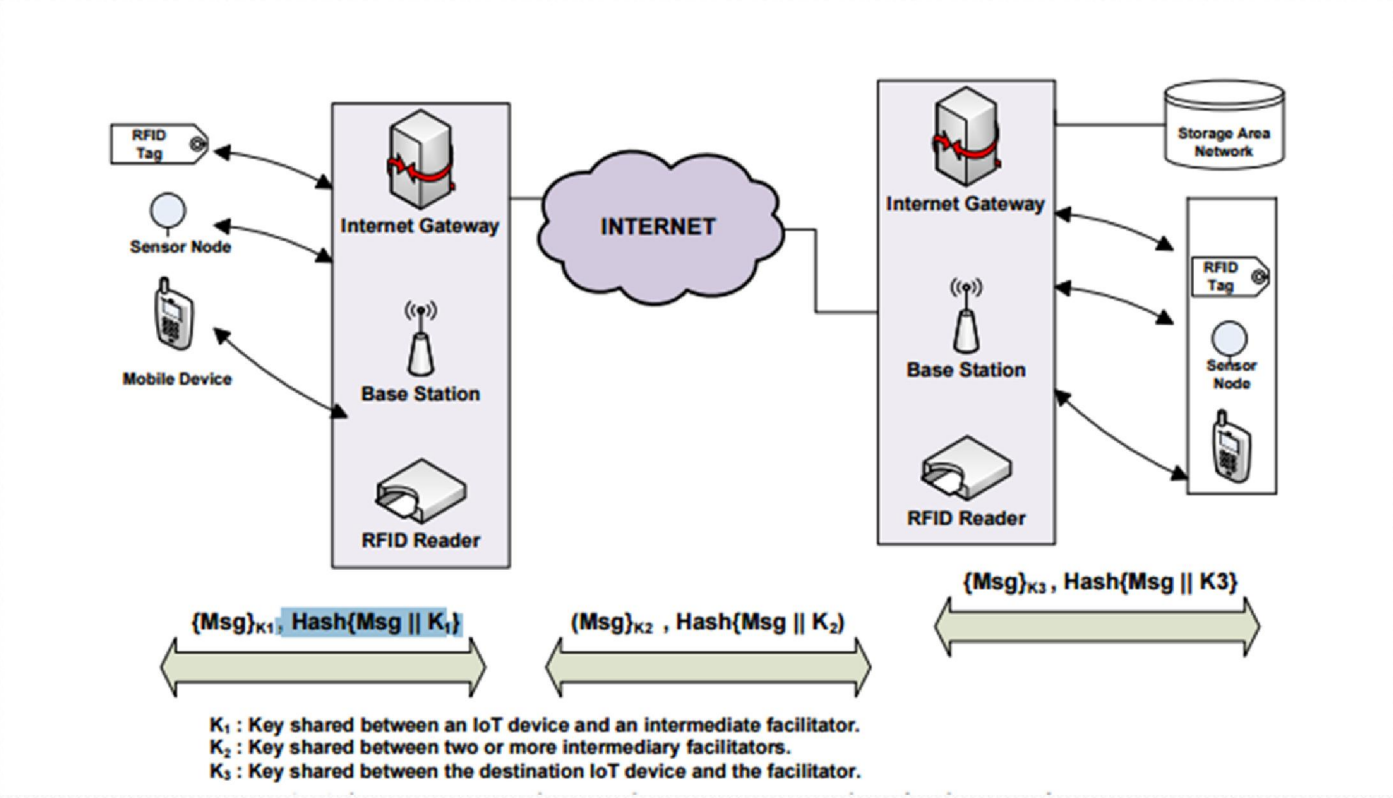
Wifi Security

- WIFI is useful for example a patient having sensor on his body can transmit the reading security to the remote health care facility.

Security of IOT infrastructure

- All devices with larger set of information processing resources are called facilitators.
- The communication between IOT devices and facilitators is secured by key K1 and MAC(message authentication code is used for data integrity and authenticity.
- Similar approach is used to secure communication channels between different facilitators with the key k2.
- The scheme used for data encryption and integrity check will use device in question.

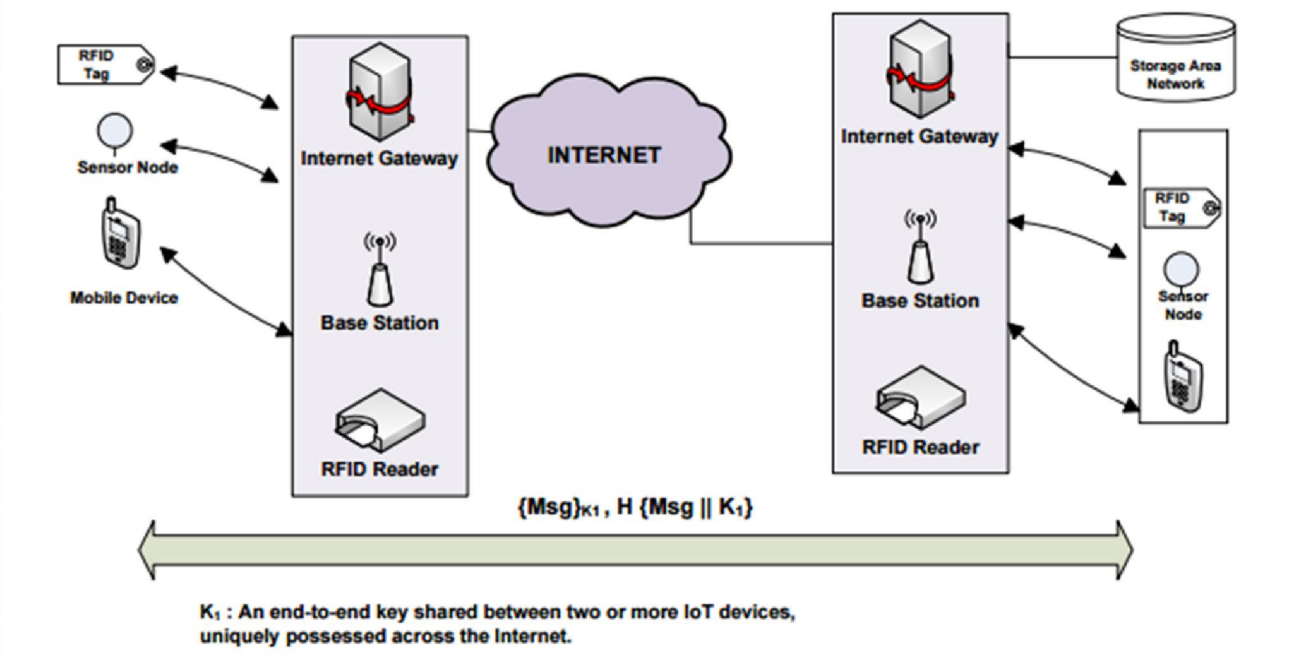
Securing IOT Infrastructure



Security IOT infrasturcture

- RFID tags used symmetric encryption and smaller key lengths
- Facilitator s have more computing resources and use public key cryptography.
- Alternative way to protect the internet of thing is a way in which all the devices possess a distinct key to identify themself in global context. It is achievable in IPV6.
- 128bit . 3.4x10^38 distinct Internet address . Can accommodate more devices. Provide end to end encryption

Security IOT infrasturcture



Criticising Paper

- The paper gives the good analysis of different security techniques used in IOT infrastructure
- Research is based on the experiments and based on these experiments we have some results.
- This research is based mostly on the data gathering from different resources. It is not own research based.
- No detailed explanation on IPV6 that how it is useful for protecting IOT infrastructure.