**An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography**

1) Healthcare Environment + Internet of Things 🡪 Provision of comfort to physicians and patients

**How**? Managing patients information, medical emergency, and etc.

2) Which **technology** to use? Radio Frequency Identification (RFID)

* There are schemes for authentication using this technology.

3) Elliptic Curve Cryptography (ECC) 🡪 It can be used for authentication.

4) Parameters for evaluating the ECC-based authentication schemes:

* Performance 🡪 Computation Cost (Running Time) and Communication Cost (Data Packet Size)
* Security

5) Usage of RFID technology 🡪 For identification of the devices and transmission of data.

6) **Goal**: A secure communication between the server and RFID tag.

7) Classification of Authentication Schemes:

* Public-Key Cryptosystem 🡪 More complicated operations.
* Non Public-Key Cryptosystem

8) Public-Key Cryptography (a.k.a. Asymmetric Cryptography):

1. A public key is used in order to encrypt the plain text. 🡪 Generation of Cipher Text
2. A private key is used in order to decrypt the cipher text. 🡪 Reconstruction of Plain Text

9) Advantages of ECC-based Authentication Schemes:

* Provision of the same security level as the non-ECC-based schemes.
* Smaller key size
* Lower computational level

10) Main components in RFID Authentication Scheme:

* RFID Tag 🡪 The location of an object identity information.
* RFID Reader 🡪 It is an interface between the other components.
* RFID Server 🡪 The source of all of the trustworthy information.

11) Three types of RFID tags:

**Passive**

* Getting power from the RFID reader through the wireless signal.
* Using backscatter modulation for data transmission.

**Semi-Active**

* Getting power from an equipped battery.
* Using backscatter modulation for data transmission.

**Active**

* Getting power from an equipped battery.
* Communicating directly with the Reader through a radio transceiver.

12) Security Requirements for RFID Authentication:

* **Mutual Authentication**: Provision of permission from both Tag and Server side.
* **Confidentiality**: Inaccessibility of the secret information for an adversary.
* **Anonymity**: The identity of tag should not be known.
* **Availability**: The information of both the tag and server should be updated.
* **Forward Security**: Inability of an adversary to trace back the last position of tag based on the previously retrieved information.
* **Scalability**: Increase in the number of tags should not increase the computation workload of server significantly.
* **Attack Resistance**: The authentication technique should be able to defend itself in confronting different attacks.

13) Classification of ECC-based Authentication Methods (based on the used number of operations):

* Heavyweight
* Middleweight
* Lightweight 🡪 It has the highest performance.

14) The story of authentication:

* An authentication session is started between the tag and server sides.
* At each side, the desired parameters are calculated and a message is constructed accordingly. The constructed message is sent to the other side through Reader for verification.
* This process is continued one or more times.
* The communication between the tag and server is established either by the tag or server decision.