**A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks**

1) **Goal**: Proposing a new method for controlling the access of “Mobile Health Networks”.

2) Conversion from Paper-Based Medical System to Electronic Healthcare System (EHS), Why?

* Universal Accessibility
* High Accuracy and Efficiency
* Low Cost
* Improving Healthcare Quality

**Important**:

* Classical EHS 🡪 Having Desktop Users
* Modern EHS 🡪 Having Mobile and Desktop Users 🡪 Mobile Healthcare Systems

Notice: Advantage of Modern EHS 🡪 Collection of data efficiently and provision of better medical services.

3) Problem of EHS 🡪 Leakage of Personal Health Record (PHR)

Solution: The personal health records should be verified, without revealing the patient identity privacy.

4) **Paper Work** 🡪 Proposing a decentralized system that leverages the attributes (or information) of the users for the purpose of authentication.

According to this system, the users authenticate each other using their attributes with considering advanced privacy requirements in their interactions. Meanwhile, the users don’t need to reveal their identities.

Notice: Common infrastructures for mobile healthcare systems are centralized. However, centralized infrastructures are not secure anymore.

5) **Threat Models**

* Impersonating real patients
* Launching identity theft attack
* Stealing and publishing patient health information
* Privacy leakage from mobile devices

6) System Storage 🡪 It contains the identity information and personal health record of every patient.

7) **Attribute**

Meaning: A feature or characteristic or someone or something.

Definition: A piece of information that determines the properties of a tag in a database.

Example: Existing symptoms, undergoing treatments, and etc.

8) Classification of Authentication Infrastructure 🡪 (a) Centralized and (b) Decentralized

9) Decentralized Infrastructure 🡪 Distributed Authentication and Direct Communication

**Important**: The users (patients and physicians) want to authenticate each other mutually in order to interact with each other, without revealing their identities. The authentication is provided using the attributes of the users.

10) Preventing Privacy Exposure 🡪 Using an encryption technique

11) **Components in this System Model**:

* Trust Authority 🡪 Responsible for key distributions for the users.
* Registration Center (e.g. hospital or clinic)
* Trust Authority has the role of certifying its qualification.
* This center provides certifications for the physicians and patients according to their provided information and attributes.

\* Patient Information Example 🡪 Disease Symptoms

\* Physician Information Example 🡪 Professional Expertise

12) Defeating Tracing Attack 🡪 Using pseudo-identities (fake identifiers) by the users

13) More Privacy Level 🡪 (a) Revealing less information and (b) Having more computation costs

14) **Active Attack Examples**

* Impersonation Attack 🡪 Pretending to be either physician or patient.
* Eavesdropping Attack
* False Data Injection Attack
* Tracing Attack 🡪 Finding a real identity based on the collected information.
* Collusion Attack 🡪 This attack is created by a group of malicious users.
* Unique Identification Attack 🡪 Example: Having only one user in a medical group.

15) **Cardinality** 🡪 The number of elements in a set as its property.

16) **Conclusion** 🡪 Using the proposed system, the patients can be diagnosed and get advices and treatments without revealing their identities.