**Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption**

1) Using Cloud Computing for Electronic Healthcare Systems (EHSs), Why?

* **Cost-Effective** 🡪 For (a) data management and storage, and (b) computational resources
* Wide-Area Mobile Access
* Reliability
* Scalability
* Elasticity and Resiliency

2) Challenges of using Cloud Computing for Electronic Healthcare Systems 🡪 Related Issues to:

* Data Security
* Patient Privacy
* Overall Performance

3) Standard Encryption Techniques 🡪 They are used for encryption/decryption of PHRs:

* Public Key
* Symmetric Key

**Deficiency** 🡪 Not suitable for EHS 🡪 Due to overlapping in accessing the information

4) **Goal**: Proposing a new technique for encrypting/decrypting the personal health records.

Important Notice 1: The technique uses the attributes of healthcare providers for encryption of the personal health records. Also, it provides an access policy for ciphertexts.

Important Notice 2: The technique uses the delivered cloud storage and computing resources by the cloud service provider.

5) Comparison between Standard Encryption Techniques:

* Public-Key Encryption
* Secure
* Not Practical 🡪 For distributing and managing large number of keys
* Symmetric-Key Encryption
* Efficient
* Not Secure Enough
* Requiring Additional Mechanism for Access Control

6) Attribute-Based Encryption

* A type of public-key encryption
* Secret Key and Ciphertext 🡪 Both dependent on specific attributes

Important Notice: A ciphertext can be decrypted only if the user key attributes match the ciphertext attributes.

In other words, the attributes of user key (e.g. living country) should satisfy the access policy of the ciphertext. In fact, each user has a specific key based on his/her attributes.

7) Elliptic Curve Cryptography (ECC)

* A type of public-key cryptography
* Using the algebraic structure of elliptic curves over finite fields
* ECC Security 🡪 Based on the hardness of the elliptic curve discrete logarithm problem
* Leveraging keys with small size
* Using less memory and processing power

8) Elliptic Curve Discrete Logarithm Problem:

* and 🡪 A Finite Field and An Elliptic Curve
* Base: and )
* Problem Definition: in

9) Bilinear Maps

* Constructing a relationship between two cryptographic groups.
* Providing the possibility of designing new cryptographic schemes.

Purpose: Conversion of a hard problem in one group to an easier problem in another group.

10) **Paper Work** 🡪 Mechanism of Proposed System:

* Creation of personal health record (PHR).
* Generation of access policies (i.e. access structure) according to the attributes of the keys of users.
* Encryption of PHR based on the generated policies.
* Uploading the encrypted PHRs into the cloud in an organized manner.

Notice 1: More Number of Attributes 🡪 More System Duration Time and Storage Overhead

Notice 2: Access Policies 🡪 An access structure over the set of all of the available attributes.

Notice 3: Each user key is specific since it is associated with specific attributes.