**Detection of Insider Attacks in Cloud-Based E-Healthcare Environment:**

-------------------------------------------------------------------------------------------------------------------------------------------------

1) **Cryptography Techniques** 🡪 Provision of a secure communication channel.

**Important 1**: They cannot provide security for the end points, which can be attacked by a malicious insider.

**Important 2**: Modification on the Personal Health Records (PHRs) 🡪 False Examination and Treatment

2) **Goal** 🡪 Proposing a detection technique for the attacks in healthcare organizations, with these features:

* Provision of a secure communication channel.
* Recognition of data modification.
* Delivering the accountability of data usage.

3) Accountability of Data Usage 🡪 Provision of transparency and reason for data usage.

**Why?** 🡪 Finding the identity of the doer of any modification on data.

4) **Watermarking Technique** 🡪 Detection of unwanted data modification.

* Meaning: Insertion of a mark to a design.
* Definition: A marker (i.e. watermark information) is embedded covertly in a signal (or data).

In other words, it is the process of hiding digital information in a carrier signal.

* Purpose: Verification of the integrity and correctness of the signal (or data).

Notice: The final signal should look alike the original signal. In fact, the insertion of watermark information should not change the original signal noticeably.

5) **Paper Work** 🡪 The proposed detection technique consists of three main components:

* A Cryptography Technique
* A Watermarking Technique
* An Accountability Framework

6) Cloud Computing Main Functions

* Storage Capability
* Computing Capability

7) Cloud Computing Challenges

* Technical 🡪 Security, Reliability, Privacy, Scalability, and etc.
* Non-Technical 🡪 Legislation and Standard, Ownership Issues, and etc.

8) Security Issues of Electronic Healthcare System:

* Privacy of User Identity
* Integrity of Data
* Authentication
* Access Control
* Secure Data Transmission
* Ability to Inspect Data Usage

9) Two Types of Data Modification Attack on Cloud-Based EHS:

* Attack within the cloud 🡪 Modification on the residing data in the cloud storage.
* Attack outside the cloud 🡪 Modification on the exited data from the cloud storage.

10) How can there be multiple modifications on Personal Health Record (data)?

**Answer**: When a patient needs to be diagnosed by multiple physicians in different hospitals. In this case, the personal health record of the patient is sent to the trusted cloud storage and is modified by each physician based on his/her diagnosis outcome.

11) **The Accountability Framework**

* The events of the users (i.e. accessing and modifying data) are logged.
* Purpose: Finding any unauthorized change in the medical records.