**Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System**

**Abstract:**

The Distributed m-healthcare cloud computing system considerably facilitates secure and efficient patient treatment for medical consultation by sharing personal health information among the healthcare providers. This system should bring about the challenge of keeping both the data confidentiality and patients’ identity privacy simultaneously. Many existing access control and anonymous authentication schemes cannot be straightforwardly exploited. To solve the problem proposed a novel authorized accessible privacy model (AAPM) is established. Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Then, based on it, by devising a new technique of attribute based designated verifier signature, a patient self-controllable multi-level privacy preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. The directly authorized physicians, the indirectly authorized physicians and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or verify patients’ identities by satisfying the access tree with their own attribute sets.

**Introduction:**

In m-healthcare social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed healthcare providers (HPs) equipped with their own cloud servers for medical consultant. However, it also brings about a series of challenges, especially how to ensure the security and privacy of the patients’ personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering and As to the security facet, one of the main issues is access control of patients’ personal health information, namely it is only the authorized physicians or institutions that can recover the patients’ personal health information during the data sharing in the distributed m-healthcare cloud computing system.

In practice, most patients are concerned about the confidentiality of their personal health information since it is likely to make them in trouble for each kind of unauthorized collection and disclosure. Therefore, in distributed m-healthcare cloud computing systems, which part of the patients’ personal health information should be shared and which physicians their personal health information should be shared with have become two intractable problems demanding urgent solutions.

A fine-grained distributed data access control scheme is proposed using the technique of attribute based encryption (ABE). Recently, a patient-centric and fine-grained data access control in multi-owner settings is constructed for securing personal health records in cloud computing. It mainly focuses on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in m-healthcare cloud computing system.

**Existing System:**

In a m-healthcare system data confidentiality is much important but in existing system framework it is not enough for to only guarantee the data confidentiality of the patient’s personal health information in the honest-but-curious cloud server model since the frequent communication between a patient and a professional physician can lead the adversary to conclude that the patient is suffering from a specific disease with a high probability. Unfortunately, the problem of how to protect both the patients’ data confidentiality and identity privacy in the distributed m-healthcare cloud computing scenario under the malicious model was left untouched.

**Disadvantages:**

* Data confidentiality is low.
* Data redundancy is high.
* There is a violation in data security.

**Proposed System:**

Proposed system for a privacy-preserving authentication scheme in anonymous P2P systems based on Zero-Knowledge Proof. However, the heavy computational overhead of Zero-Knowledge Proof makes it impractical when directly applied to the distributed m-healthcare cloud computing systems where the computational resource for patients is constrained. Suggested patients have to consent to treatment and be alerted every time when associated physicians access their records and also our proposed system is a patient-centric and fine-grained data access control in multi-owner settings is constructed for securing personal health records in cloud computing.

Our proposed m-healthcare system mainly focuses on the central cloud computing system which is not sufficient for efficiently processing the increasing volume of personal health information in m-healthcare cloud computing system. in distributed m-healthcare cloud computing systems, all the members can be classified into three categories: the directly authorized physicians with green labels in the local healthcare provider who are authorized by the patients and can both access the patient’s personal health information and verify the patient’s identity and the indirectly authorized physicians with yellow labels in the remote healthcare providers who are authorized by the directly authorized physicians for medical consultant or some research purposes. They can only access the personal health information, but not the patient’s identity. For the unauthorized persons with red labels, nothing could be obtained.

 The security and anonymity level of our proposed construction is significantly enhanced by associating it to the underlying Gap Bilinear Diffie-Hellman (GBDH) problem and the number of patients’ attributes to deal with the privacy leakage in patient sparsely distributed scenarios. More significantly, without the knowledge of which physician in the healthcare provider is professional in treating his illness, the best way for the patient is to encrypt his own PHI under a specified access policy rather than assign each physician a secret key. As a result, the authorized physicians whose attribute set satisfy the access policy can recover the PHI and the access control management also becomes more efficient.

**Advantages:**

* M-healthcare system is fully controlled and secured with encryption standards.
* There is no data loss and data redundancy.
* System provides full protection for patient’s data and their attributes.

**Modules:**

**E-healthcare System Framework:**

E-healthcare System consists of three components: body area networks (BANs), wireless transmission networks and the healthcare providers equipped with their own cloud servers. The patient’s personal health information is securely transmitted to the healthcare provider for the authorized physicians to access and perform medical treatment. Illustrate the unique characteristics of distributed m-healthcare cloud computing systems where all the personal health information can be shared among patients suffering from the same disease for mutual support or among the authorized physicians in distributed healthcare providers and medical research institutions for medical consultation.

**Authorized accessible privacy model:**

Multi-level privacy-preserving cooperative authentication is established to allow the patients to authorize corresponding privileges to different kinds of physicians located in distributed healthcare providers by setting an access tree supporting flexible threshold predicates. Propose a novel authorized accessible privacy model for distributed m-healthcare cloud computing systems which consists of the following two components: an attribute based designated verifier signature scheme (ADVS) and the corresponding adversary model.

**Security Verification:**

The security and anonymity level of our proposed construction is significantly enhanced by associating it to the underlying Gap Bilinear Diffie-Hellman (GBDH) problem and the number of patients’ attributes to deal with the privacy leakage in patient sparsely distributed scenarios. More significantly, without the knowledge of which physician in the healthcare provider is professional in treating his illness, the best way for the patient is to encrypt his own PHI under a specified access policy rather than assign each physician a secret key. As a result, the authorized physicians whose attribute set satisfy the access policy can recover the PHI and the access control management also becomes more efficient.

**Performance Evaluation:**

The efficiency of PSMPA in terms of storage overhead, computational complexity and communication cost. a patient-centric and fine-grained data access control using ABE to secure personal health records in cloud computing without privacy-preserving authentication. To achieve the same security, our construction performs more efficiently than the traditional designated verifier signature for all the directly authorized physicians, where the overheads are linear to the number of directly authorized physicians.

**Conclusion:**

A novel authorized accessible privacy model and a patient self-controllable multi-level privacy preserving cooperative authentication scheme realizing three different levels of security and privacy requirement in the distributed m-healthcare cloud computing system are proposed, followed by the formal security proof and efficiency evaluations which illustrate our PSMPA can resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.