

**CHENNAI – PONDICHERRY**

**Cloud-based Fine-grained Health Information Access Control Framework for Lightweight IoT Devices with Dynamic Auditing and Attribute Revocation**

**Abstract:**

The eHealth trend has spread globally. Internet of Things(IoT) devices for medical service and pervasivePersonal Health Information (PHI) systemsplay important roles inthe eHealth environment. A cloud-based PHIsystem appearspromising but raises privacy and informationsecurity concerns. We propose a cloud-based fine-grained health information access control framework for lightweight IoT devices with data dynamics auditing and attribute revocation functions. Only symmetriccryptographyis required for IoT devices, such as wireless body sensors. A variant of ciphertext-policy attribute-based encryption, dual encryption,and Merkle hash treesare used to support fine-grained access control, efficient dynamic data auditing, batch auditing,and attribute revocation. Moreover, the proposed scheme also definesand handlesthe cloud reciprocityproblem wherein cloud service providerscanhelp each other avoid finesresulting fromdata loss. Security analysis and performance comparisons show thatthe proposed scheme is an excellent candidate for a cloud-based PHI system.

**Existing System:**

One solution for aneffective PHI system is to adopt a cloud-based storage tomitigatethe burden of building and mainte-nancecost. However, outsourced PHI faces the challenge of security and privacy issues, for instance, how to ensure that only the authorized requester can access the sensitive PHI or to prevent asemi-trusted Cloud Service Provider (CSP) from leakingstored information. In addition, the Health Insurance Portability and Accountability Act (HIPAA) comprisesa list of privacy requirements orprotectingconfidentiality fromthe data storage server. Data integrity at asemi-trusted CSP isan-other important concern. CSPsfacing occasional catastrophicfailures mightdecide to hide data errors from a patient for their ownbenefit. Although the data owner backs up hisor her extremely important data in multiple CSPs, some CSPs might exercisemutual aid to avoid the huge costof dataloss.We call thisthe*cloud reciprocityproblem*. The fact that a stored PHI would not only be accessed by medical workers but also up-dated by the patientrequires support fordata integrity verifi-cation for dynamic data operations.

**Proposed System:**

We propose a fine-grained health information access control framework in the cloud for lightweight IoT deviceswith data dynamics auditing and attribute revocation functions. Regard-ingsecurity and privacy, we useCiphertext-Policy Attribute-Based Encryption (CP-ABE)to perform fine-grained access control on thepart of a decryption keythatis used to decrypt sensitive patient PHI.Basically, each Data Access Requester (DAR)hashis/her ownprivate keys associated with a set of attributes, andan essential decryption parameter TSK specifies an access policy over a defined universe of attributes. DAR can extract TSK todecrypt the encrypted PHI if and only if his/her attributes satisfy the access policy.