**A SIMPLE POLICY UPDATE SYSTEM FOR SHARING OUTSOURCED PERSONAL HEALTH RECORDS**

**ABSTRACT**:

With high flexibility and accessibility of data outsourcing environment such as cloud computing environment, several healthcare providers implement electronic personal health records (PHRs) to enable individual patients to manage their own health data in such resilient and scalable environment. However, PHRs contain highly sensitive information of which the security and privacy issues are the critical concern. Besides, PHRs owners should be capable to flexibly and securely define their own access policy for their outsourced data. In addition to the basic authentication feature, existing commercial cloud platforms usually provide symmetric or public key encryption as an optional feature to support data confidentiality for their tenants. However, such traditional encryption schemes are not suitable for data outsourcing environment because of high key management overhead of symmetric encryption and high maintenance cost for handling multiple copies of ciphertext for public key encryption solution. In this paper, we design and develop a secure and fine-grained access control scheme with lightweight access policy update for outsourced PHRs. Our proposed scheme is based on the ciphertext policy attribute-based encryption (CP-ABE) and proxy reencryption (PRE). In addition, we introduce a policy versioning technique to support the full traceability of policy changes. Finally, we conducted the performance evaluation to demonstrate the efficiency of the proposed scheme.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * These factors will also increase the complexity of the data collection. Most existing NMF-based dynamic topic model methods treat each potential topic as an independent element, and ignore the intersection of each topic and the relationship between them, thus limiting the expressive power of these models. * Hierarchical structure is the core feasible solution to overcome this defect. However, most of the general existing hierarchical topic models are static models, which cannot meet the requirements of detecting topics in the text stream. | * Therefore, researchers have proposed a method to eliminate redundant blocks. Each non-leaf node optimizes the layout of its child nodes through the variation circle arrangement method. Here, each child node can have a different weight value, and the weight value reflects the area ratio of the circle corresponding to these child nodes in the circle of the node. * Each node of hierarchical data is often associated with a set of the node attributes, which can be combined according to application requirements for weight assignment or weight assignment directly by user interactively. |
| **EXISTING ALGORITHM: -**  **Data Analytic Model** | **PROPOSED ALGORITHM: -**  **Data Mining with Layered Model** |
| **ALGORITHM DEFINITION: -**  We present the analytic model that is weight assignment of each node, the layout algorithm recursively deals with the circle layout of nodes at each level in a breadth-first manner from the root node. Here, the sibling nodes of the same parent node maximize their corresponding circles within the circle of their parent node, and do not coincide with each other, so as to improve the space utilization rate as much as possible | **ALGORITHM DEFINITION: -**  Fixed-length block redundancy cannot be adjusted and optimized intelligently according to the content of the file itself, which makes this method very inefficient for the file insertion and deletion problems, and the effect of redundancy elimination is very poor. Therefore, researchers have proposed a method to eliminate redundant blocks. Each non-leaf node optimizes the layout of its child nodes through the variational circle arrangement method. |
| **DRAWBACKS: -**   * System can participate in the reading, writing, verification and consensus process of data. * The development of Internet technology and the Internet + financial industry. * Factors affecting and also restricting financial activities have become more complex. | **ADVANTAGES: -**   * Can participate * Development * Affecting and restricting |

**MINIMUMSYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUO.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE

**System Architecture:**

