ISSN:0975-9646

# Providing Improved Response in Healthcare Domain by Using Knowledge Based HSOA

T.Silambarasan [1], V. Udhaya kumar[2]

*[1]PG Scholar , [2]Assistant Professor*
*Computer Science and Engineering Department,*
*PRIST University, Thanjvur – Pondicherry Campus.*

**Abstract— The grid technology is used to implement tending services-oriented style (HSOA) for Virtual Organization (VO) Management in tending environments. Management of users, assignation of roles to users, assignation of privileges to roles, and definition of resources access policies unit of measurement totally different tasks that will be done as a region of this methodology, thus adding to its efficiency. The VO management services unit of measurement provided as an area of the privilege management infrastructures (PMI), that supports access management to tending resources at intervals the HSOA. Application of traditional, secure, discipline vogue techniques makes the PMI completely open and sensible. The introduced linguistics technologies in decision points for access management. this permits management of a high degree of descriptors by suggests that of anthologies and put together infers higher mental process through rules and reasoners.**

**Keywords—** ***grid technology, Virtual Organization, privilege management infrastructures, anthologies***

## I.INTRODUCTION

Grid computing is a term referring to the combination of computer resources from multiple administrative domains to reach a common goal. Grid computing combines computers from multiple administrative domains to reach a common goal, to solve a single task, and may then disappear just as quickly the goal of Grid computing is to create a “virtual organization” across one or more physical organizations or “administrative domains.” These virtual organizations are facilitated by common solutions for resource management, data management and access, application development environments, and information services. The approach for designing a system providing services to both end-user applications and other services distributed in a network is often called service-oriented architecture (SOA). A Service-Oriented Architecture (SOA) is a set of principles and methodologies for designing and developing software in the form of interoperable services Service requires loose coupling of services with operating systems, and other technologies that underlie applications. SOA separates functions into distinct units, or services, which developers make accessible over a network in order to allow users to combine and reuse them in the production of applications.

## II.KNOWLEDGE- BASED SYSTEM

The implementation of Policies through the set of services like PIP, PEP and PDP improves data security. Also, the System in upgraded with Knowledge-Based System. This will promise a better response to the requesting users. Knowledge based systems are artificial intelligent system working in a domain to provide intelligent decisions with justification. The Benefits includes avoidance the limitation of worst response, Security is improved by tuning the PMI, It also gives a grater satisfaction to the dependent, Provides appropriate service based on the user Privileges.

The Grid server will maintain all the information of doctor’s list, patient’s list, domain list, and visitor’s list. The domains are created by the server administrator. The person who wants to enter into the service will give the IP address of the grid server. Once the dependent enters into the grid service, The dependent have to identify himself/ herself as doctor or patient or visitor. After which the registration begins. If the dependent is a fresher, he/she has to sign up first. After signing up, the dependent name will be displayed on the server. Now the server will authorize the dependent to get signed in successfully. The database holds all the information that to be provided to the dependant. Based on the type of user, the system will assign privilege to that particular user. Now available resources are not able to support such a thing, especially if we consider the frequency of health care treatments across the entire state and that every treatment has to be recorded in the system, with bunch of other related data. Besides, this approach implies unexceptionable network connections between all tree nodes, as inside of them, which is not the case anywhere in the world yet Knowledge-Based system is developed to find out the most closest alternative of the requested data. As the user request for a data, the system will search for the data in the database, if the data is available then it is returned, if not, the Knowledge Base will play its role to generate the alternative data from same database and will return the same to the requested user. This emerging approach for explicit data and policy management improves the response. These new capabilities will ensure a more trust worthy grid infrastructure.

## III.MODULES

### A.AUTHENTICATION AND AUTHORIZATION MODULE

Authentication is the mechanism whereby systems may securely identify their users. Authorization, by contrast, is the mechanism by which a system determines what level of access a particular authenticated user should have to secured resources controlled by the system.

The Grid server will maintain all the Information of Doctor's List, Patient's List, Domain List, and Visitor's List. The Domain's are created By the Server administrator. In Fig 6.1 the Person who wants to enter into the service will give the IP address of the Grid server. Once the dependent enters into the Grid service, The Dependent has to identify himself/ herself as Doctor or patient or visitor. After which the registration begins. If the Dependent is a Fresher, he/she has to sign up first. After signing up, the dependent name will be displayed on the Server. Now the Server will authorize the dependent to get signed in successfully

Authorization is the function of specifying access rights to resources, which is related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define access policy. For example, human resources staff are normally authorized to access employee records, and this policy is usually formalized as access control rules in a computer system. During operation, the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected). Resources include individual files' or items' data, computer programs, computer devices and functionality provided by computer applications. Examples of consumers are computer users, computer programs and other devices on the computer.

Access control in computer systems and networks relies on access policies. The access control process can be divided into two phases

1. Policy definition phase where access is authorized, and
2. Policy enforcement phase where access requests are approved or disapproved.

Authorization is thus the function of the policy definition phase which precedes the policy enforcement phase where access requests are approved or disapproved based on the previously defined authorizations

### B.PEP &PDP SERVICE MODULE

In this module the policy enforcement point (PEP) services directly related to resources belong to the infrastructure layer; and policy decision point (PDP) services, all belong to the generic service layer; finally, the credential repository and the policies semantic knowledge base are part of healthcare domain services layer because of their functionality.

Another important point included is the consideration of separate and distributed policy information points (PIP). Each one follows its own functional protocol (centered on a particular kind of at-tributes, receiving requests, and sending information) and it is connected to the related knowledge base. Following this trend the proposed infrastructure replaces centralized components of the services that can be distributed and decomposed in other simpler services. From an architectural point of view, shows services from different layers of the HSOA

The policy enforcement point (PEP) services directly related to resources belong to the infrastructure layer; services as context handler easing distribution and location are part of middleware layer; resource and environment knowledge bases, PIP services, and policy decision point (PDP) services, all belong to the generic service layer; finally, the credential repository and the policies semantic knowledge base are part of the healthcare domain services layer because of their functionality and content are specifically defined to this domain.

### C.CONTEXT HANDLER SERVICE MODULE

In this module the context handler services to distribution and location are part of middleware layer. The subject PIP service information is stored into Credential Repository. Here PIP services provider (environment PIP service and resource PIP service. The each service provides the Resource Knowledge base service on context handler

The context handler service belongs to middleware and it deals with the distribution and location of the different services thus, it can be implemented in several ways and even it could be integrated in PDP and PIP services. For the sake of simplicity, in the proposed infrastructure performs tasks for discovering and communicating between the different PIP, PEP, and PDP services To achieve the variability degree required by access control policies, we have modeled an ontology of healthcare domain fulfilling all the potential features of categorization of resources. By using this ontology, the administrator (potentially the SoC) can have a versatile control over the access to resources through the potential actors who can access, the nature of the information, creation dates, authors, physical allocation of access, purpose of use, etc

The job of the context handler is to generate an authorization request based on the authentication data and the service request details from the user and query the PDP. Depending on the response from the PDP Permit, Deny, Indeterminate or Not-Applicable. The context handler will return program control to the gatekeeper with the appropriate return code. PDP service receives all the information from PIP services through context handler service

### D.TECHNIQUES

#### 1. Policy Enforcement Point (PEP)

The digital representation of the Policy is provided by the policy Information Point to the policy Decision Point which then passes the decision to the Policy Enforcement Point where the access is permitted or denied. Policy information point is the Point which can provide external information to a PDP, such as LDAP attribute information. A policy is simply, an official or prescribed plan or course of action. A policy itself provides no enforcement, no compliance and no enforcement The PEP will give the Policy Decision Point (PDP) the job of deciding whether or not to authorize the user based on the description of the user's attributes. The PEP will let the user know whether or not he has been authorized to access the requested resource.

The PEP's main function is to grant or deny user access to the resource and enforce workflow obligations or constraints on the interaction. The PEP can also support user authentication, by checking the status of a user's credentials and verifying authentication assertions

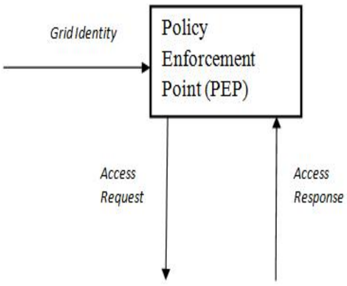

**Fig. 1 policy enforcement point**

## 2. Policy Decision Point

Evaluates access request decision queries issued by enforcement points. PDP has access to the set of policies and evaluates access requests against applicable policies. Policy Decision Point (PDP) is the point where policy decisions are made. PDP services are all independent elements, adding flexibility to the management of VO (Virtual organization).

An efficient PDP service is implemented in Privilege and Role Management Infrastructure Standards. Its main entities are an authorization policy, a set of users, a set of administrators (attribute authorities) who assign roles/attributes to users. A set of resources that are to be protected, a set of actions on resources, a set of access control rules, and optional obligations and constraints.

The primary function of the PDP is to render an access control decision based on a policy. This is calculated through access control decisions based on the security context of the interaction between the user and the application or resource being protected. The security context is comprised of access control parameters including policies, user attributes, resource metadata, and environment attributes. The PDP can retrieve the access control parameters from sources at various levels of the enterprise to render a decision.

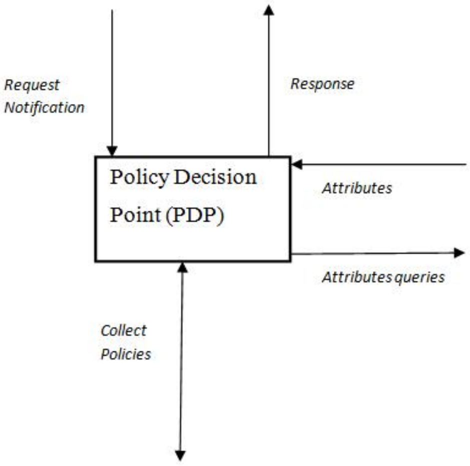

**Fig. 2 Example of an image with acceptable resolution**

## 3. Context Handler Service

The context handler service belongs to middleware and it deals with the distribution and location of the different services; thus, it can be implemented in several ways and even it could be integrated in PDP and PIP services.

The context handler is the only application dependent component of the system. It uses the Globus gatekeeper authorization call-out interface. The job of the context handler is to generate an authorization request based on the authentication data and the service request .Depending on the response from the PDP Permit Deny, Indeterminate or Not-Applicable. The context handler will return program control to the gatekeeper with the appropriate return code. PDP service receives all the information from PIP services through CHS.

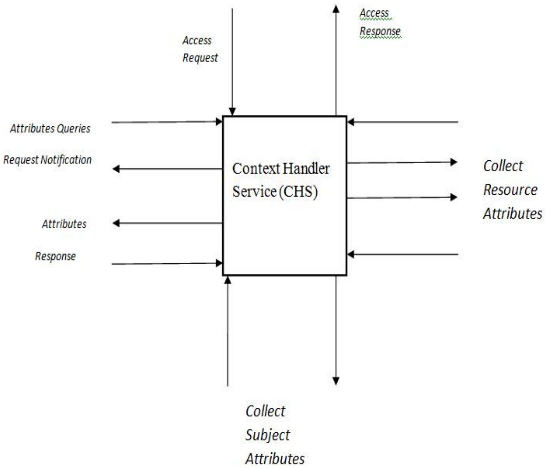

**Fig. 3 context handler service**

### 4. Policy Information Point

The policy information points (PIP) it's contain own functional protocol (centered on a particular kind of attributes, receiving requests, and sending information) and it is connected to the related knowledge base. Policy information point (PIP) is The system entity that acts as a source of attribute values In the system it is a entity that acts as a source of attribute values.

To use a policy information point in Health-care environment, the system must be using the runtime security services server or client that is configured to perform local mode authorization as your policy decision point

Policy Information Point determines the kind of information collected, created, organized, stored, accessed, disseminated and retained. Who can use the information, whether there will be charges for access, and the amount charged, is also covered. Usually associated with government information, information policy also establishes the rules within which private information providers and the media operate

System entity that acts as a source of attribute values for a Policy set. A Policy set can be a set of policies, other policy sets, a policy-combining algorithm and a set of obligations or may be a component of another policy set

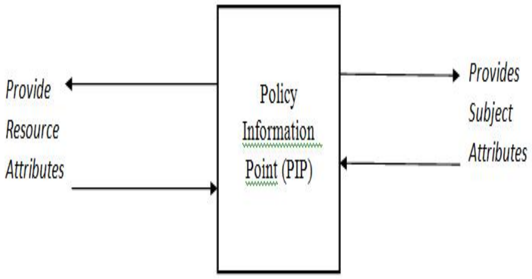

**Fig. 4 Policy Information Point**

The PIP retrieves access control policies from a policy store. Typically, the PDP will use the PIP to request policies pertaining to the security context of a transaction. Rules typically are utilized in a collection, known as Policies to be called up by the PIP.

## IV.CONCLUSIONS

Knowledge-Based system combined along with Health-care service oriented Architecture to provide improved performance. This Knowledge-Based HSOA will generate the better alternative data at times when the system finds there is no match of the requested data. The service PEP, PDP and PIP improves the security of the data. It blocks unauthorized access to the data's. Context handler Service serves as a better interface between the user and the Database, which also allows secured data transfer. This emerging approach for explicit data and policy management improves the response. These new capabilities will ensure a more trust worthy Grid infrastructure

## REFERENCES

1. Privilege management Infrastructure for Virtual Organization in Healthcare Grids IEEE transaction on information technology in biomedicine, vol 15, no 2, March 2011.
2. Health Informatics—Privilege Management and Access Control, ISO 22600-1,2, 2006.
3. Health Informatics—System of Concepts to Support Continuity of Care Part 1: Basic Concepts, European Committee for Standardization, CEN/TC 251, EN 13940-1, 2006.
4. D. J. Power, E. A. Politou, M. A. Slaymaker, and A. C. Simpson, "Towards secure grid-enabled healthcare," Softw. – Practice Exp., vol. 35, no. 9, pp. 857–871, 2005.
5. The Systematized Nomenclature of Medicine (SNOMED) [Online]. Available : http://www.ihtsdo.org/snomed-ct/.
6. Health Informatics—Electronic Health Record Communication—Part 4: Security, ISO 13606-4, 2007.