# Secure Knowledge Sharing by using Role Attribute based Encryption

Mrs. C. Gomathi
Assistant Professor
Department of IT/CSE
Anna University BIT campus,
Tiruchirappalli, India.

Dr. V. Rajamani
Professor & Principal
Department of ECE,
Vel Tech Multi Tech Engineering College,
Chennai, India.

Ms. M. Priya
M.E student
Department of Software Engineering,
Anna University BIT campus,
Tiruchirappalli, India

***Abstract*— Knowledge sharing is one of the operations in knowledge management that can be used to improve the performance of the organization. Knowledge mainly used to improve the performance of the organization. Healthcare knowledge is used to improve the quality of service provided by the organization and knowledge is mainly helpful to support decision making system. In this work, cancer patient's dataset is taken from UCI repository and each factor is analyzed. Fuzzy logic is applied to consider weight age for factors which are important to determine the cancer. In fuzzification process, Trapezoidal membership function is elected to convert crisp values to fuzzy values. Fuzzy rules are formed to predict the relationship between the factors. By assisting fuzzy rules, ontology graph is constructed to represent the relationship between the factors. Ontology graph is the most conventional technique to accomplish the knowledge from the data set. The acquired knowledge needs to be shared in cloud environment to make accessible the knowledge everywhere. There are still many security and privacy challenges impeding the wide adoption of cloud computing. Encryption algorithms are used to address these security challenges. Attribute based encryption algorithm is preferred to overcome the security issues while sharing the knowledge in cloud environment. This study shows that the result of patient knowledge represented in the form of OWL ontology and shared securely using Attribute based encryption algorithm.**

***Keywords— Ontology, Attribute based encryption, cancer.***

## I. INTRODUCTION

Healthcare system is one of the knowledge plentiful domains. Healthcare knowledge is not just a resource. It is a „service" point-of-care decision support. It is mostly employed to support clinical decision-making, patient management services, such as care planning, alerts. Healthcare system contains different types of knowledge such as patient knowledge, practitioner knowledge, medical knowledge, resource knowledge, organizational knowledge, etc. This work considers only patient knowledge by the analysis of cancer patient"s characteristics.

Cancer is the speedy creation of abnormal cells that grow afar their usual boundaries, and which can then attack any adjoining parts in the body and spread it to other organs. [1] Cancer facts are listed out in world health organization as follows; there are more than 100 types of cancer that affect any part in the body. The most commonly diagnosed cancer worldwide is lung cancer. The maximum common bases of cancer death are listed out in the following table 1.1.

| Cancer | Death rate | Percentage of total |
|---|---|---|
| Lung cancer | 1.61 million | 18.2 |
| Breast cancer | 1.38 million | 10.9% |
| Stomach cancer | 738000 | 9.7 |
| Liver cancer | 696000 | 9.2 |

Table 1.1 Cancer death rates

The second leading cause of death among women is breast cancer, as it comes directly after lung cancer. Cancer risk factors are considered as physical inactivity, unhealthy diet, Tobacco and alcohol use etc. Tobacco use is considered as the single largest preventable source of cancer in the world causing 22% of cancer deaths.

Fuzzy logic is applied to consider weight age for factors which are important to determine the cancer. Fuzzy rules are generated based these weight ages of each factors. By using these rules ontology graph was constructed and it shows relationships among these factors. Ontology graph provides the knowledge about relationship between symptoms of cancer disease to make diagnosis easier. Ontology graph is employed to represent the knowledge in semantically rich format. It has been effectively used in the semantic web domain for the purpose of achieving a complete and common machine-readable understanding. Ontology is conceptual model that affords a controlled vocabulary for the explanation of concepts, each with an explicitly defined semantics in machine-readable language. Ontology aims to capture consensual knowledge by a group of people and may be reused across various applications.

The captured knowledge is needed to share in cloud environment to make easily available the knowledge everywhere. Knowledge can be shared for healthcare practices to achieve high levels of care quality, patient medical
information privacy, and cost-effectiveness. These high levels of quality, privacy and cost-effectiveness can be attained through the collaboration among the users, clinicians and experts. Collaboration must overcome the security challenges while sharing the knowledge in cloud environment. Encryption can defend confidentiality of messages. But other techniques are still required to protect the authenticity and integrity of a message. Encryption algorithms are used to overcome the security challenges. Attribute based encryption algorithm is chosen to conquer the security issues while sharing the knowledge. Attribute-Based Encryption allows the encryptor to set a policy that describes who must be able to read the data. In an attribute-based encryption system, private keys allotted by an authority are related with sets of attributes and cipher texts are associated with formulas over attributes.

## II. LITERATURE SURVEY

### A. *Cancer statistics*

World Health Organization[1] estimated cancer occurrence worldwide in the year of 2012 and listed out it as there were 14.1 million cancer cases, 8.2 million cancer deaths and 32.6 million people living with cancer. Lung cancer is the leading common cancer in the world for several years and it is the most common reason of death from cancer worldwide. There are calculated to be 1.8 million new cases in 2012 (12.9% of the total). Lung cancer is mainly common cancer in men worldwide. Breast cancer is the second world level common cancer and frequent cancer amongst women. Breast cancer estimated as 1.67 million cancer cases diagnosed in 2012(25% of all cancers) and stated as fifth cause of death from cancer overall. Stomach cancer estimated as almost one million new cases in 2012(952000 cases, 6.8% of total) .It is the third leading cause of cancer death in both sexes worldwide (723,000 deaths, 8.8% of total).

### B. *Ontology*

Ontology is the fundamental form of representation knowledge about the real world. In the review of computer science, Ontology has various meanings:

i. Ontology is defined as “a formal, explicit specification of a shared conceptualization”. [9]

ii. Ontology is a symbolic representation of the knowledge about the object, object properties, class of objects and relations between objects to represent knowledge of the application domain. [16]

iii. Ontology is used to express knowledge in certain domain. Ontologies consist of hierarchical definitions of important concepts in a domain and description of the properties of each concept [2].

### C. *Web Ontology language (OWL) Format:*

Web ontology language (OWL) is a Web-based ontology language that was mainly designed for the reasons of integration and interoperability-related documents on the Web. OWL can offer additional vocabulary with a formal semantics [15]. OWL can describe the semantics of the property and the class of a document, as well as how the association. OWL has three categories of languages, namely OWL Lite, OWL DL, and OWL Full.

## III. RELATED WORK

In 2008, Yang and Chen [6] pointed out how to enhance knowledge sharing through a social network-based collaboration support. Knowledge sharing has been a motivation for participation in virtual communities. They discussed the difficulty in finding relevant content and collaborators to interact while sharing knowledge in a P2P network. They suggested social network-based collaboration, support to knowledge sharing that helped people find relevant content and knowledgeable collaborators who are willing to share their knowledge. In [2], Furkh Zeshan and Radziah Mohamad proposed ontology clarifies the concepts and the relationships among these concepts in the emergency domain. In their study, they discussed an advanced methodology service-oriented architecture (SOA) that can be used for developing dynamic, flexible, loosely coupled, cost-effective applications. SOA relies on services that handle complexity and heterogeneity by using ontologies. This ontology was mainly helpful for the effective handling of IT-based healthcare system problems especially during an emergency.

According to [3], A. Alesanco et al suggested ontology-based system that comprises for improving usage and management of items in health care centers. By describing the features of each product and its potential usage, the proposed system can be employed as a rich source of shared knowledge to assess clinical personnel concerning the selection of items. Sharing and learning knowledge described in powerful way to improve personnel safety and resource management in hospitals. Knowledge used in decision making system to improve the usage of each item. Decisions were predicted to be made based on multiple-user experience instead of individual experience. Correct management and usage of materials will have a helpful impact on health care costs and, most important, on clinician and patient safety. Argyroula Christopoulou et al [4] developed a framework for Sharing Knowledge and Integrated Information in Radiotherapy

(SKIIR) for medical physicists involved in Therapeutic Radiological Physics. The proposed SKIIR was mainly designed for sharing knowledge based on specific cases of treating patients with cancer. It described a framework focusing on treatment planning and knowledge codification. EPatCare® software tool used to allow viewing or creating patient cases. This system mainly focused on a representative of knowledge captured concerning a case and the related treatment plan. In [8] Amir Zidi et al designed a novel ontology-Based Personalized Retrieval model using the Case Base Reasoning (CBR) tool. Aida Valls et al [5] used the ontology to explain the organizational knowledge of complex healthcare. They defined the roles of the ontology in the customization of the system. Healthcare medical entities are expressed in the form of ontological classes which organize hierarchies, properties and semantically rich class restrictions.

In the above mentioned work, none of the researches has focused on confidentiality of knowledge, while sharing

between the practitioners and patients. The idea of B. Fabian et al [10] was preferred to overcome the security challenges. They presented role based access control mechanism. In this paper, we propose the secure way of patient prior diagnose service with the help of ontology for such knowledge sharing and communication.

## IV. RESEARCH WORK

### A. *Workflow of the methodology proposal*

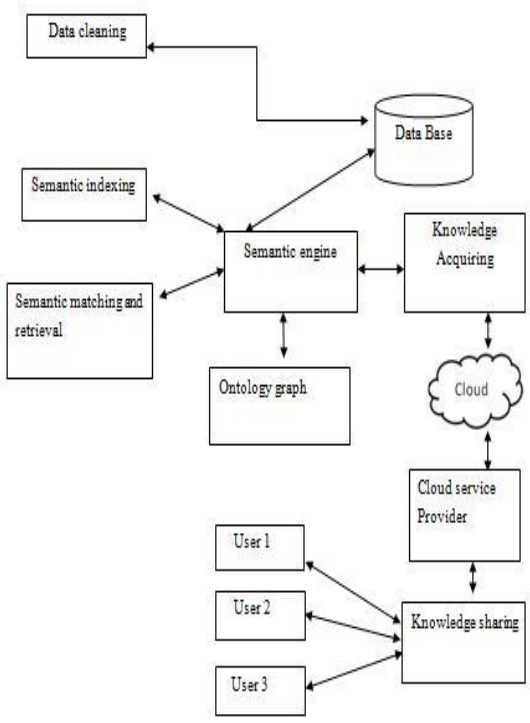


***Figure 1: Workflow of the methodology proposal.***

### B. *Methodologies*

#### i. *Preprocessing*

Data preprocessing is one of the most critical step which deals with the preparation and transformation of the initial dataset. Cancer dataset is collected from UCI machine learning repository website which contains missing values, inconsistent and redundant data. These inconsistent data is removed by using data cleaning and transformation method. In data cleaning fill up the missing values by zero, remove inconsistent data and select the relevant attribute. Missing values can be done in various ways such as fill up the missing values by simply ignoring the tuple, fill in the missing values manually, use a global constant to fill in the missing value, attribute mean to fill in the missing value, attribute mean for all samples belonging to the same class as the given tuple, the most probable value to fill in the missing value.

#### ii. *Knowledge acquisition*

Fuzzy logic algorithm is used to construct rules for acquiring knowledge. Trapezoidal waveform
membership function is used to derive the rules. Fuzzy rule consists of if and then part of extracted knowledge. Rules are generated from the dataset to make decision support system. Based on these rules weight age is assigned to the symptoms.

*Proposed Algorithm*

Input: List of attribute values from $p_1$to $p_n$
Output: Prediction of Class Label

Begin Procedure
fuzzy

{

For all attribute pi=1to n do

Trape($p_i$) //Apply trapezoidal membership function

For all i=1to n do //Build Rule Base For all
j=i+1 to n do

For all k=1 to 2 do $r_l$ =if $p_i$
or $p_j$ then $c_k$;

Combine the rules $r_l$;

For $r_l$=1 to n do //Assign Weightage to the rule

$r_l=W_m$; $m\epsilon[0,1]$

Return fuzzy value;

//Apply Robust Ranking defuzzification
Return $c_k$;

}

End

*iii. Ontology construction*

OWL (Web Ontology Language) is the language used for construct the ontology for cancer disease. Protege4.2 software tool is used for construct the ontology. Ontology represents the knowledge of cancer is used to make decision about the disease. Ontology represents the knowledge in terms of graph and provides detail about hidden relationship between symptoms. Query has been applied to ontology graph.

*iv. Graphical user interface*

User interface is the interface used between user and service provider. Authentication process, query retrieval, and query responses are done through user interface. User interface provides user-friendly look and feel to the user. Java swing is used for creating the user interface. Graphical user interface get the input from the user and send it to the semantic engine. Semantic engine search the relevant result for the user query from the database. Java and ontology in protégé 4.2 connectivity is provided by OWL API (Web Ontology Language Application Programming interface). The OWL API is a Java API and reference implementation for creating, manipulating and serializing OWL ontologies.

User enters the details such as symptoms, factors in the form. Example name, age, diet, gender etc., are entered through user interface.

*v. Query retrieval*

SPARQL query is used in query processing. It is RDF-based querying languages to support semantic search. Semantic indexing and matching process is taken place in query retrieval. OWL DL-based semantics can generally provide more exact solutions. Expressive OWL query languages are needed to build its DL semantics and supports comprehensive querying of OWL. It allows direct querying of OWL classes and properties. Semantic matching is done by s-match algorithm. In this algorithm semantic matching is done between two trees or graphs.CL matrix represents the relations holding between concepts of labels and CN matrix represents the strongest relations holding between concepts of nodes. These two matrices provide the output for the matching algorithm.

*vi. Secure sharing*

Collaboration between users and clinicians needs sharing of knowledge to provide better patients care service. The knowledge is acquired by using semantic matching and retrieval. The acquired knowledge is stored in cloud. This stored knowledge can be accessed by only authenticated users and clinicians. In cloud storage, there is reserved space allocated for each user. Every user authenticated before accessing the reserved space. This authentication process is done by service provider. Authenticated users can have unique login id and password. Attribute based encryption algorithm is used between the user and server to provide secure access of knowledge.

## V. RESULTS

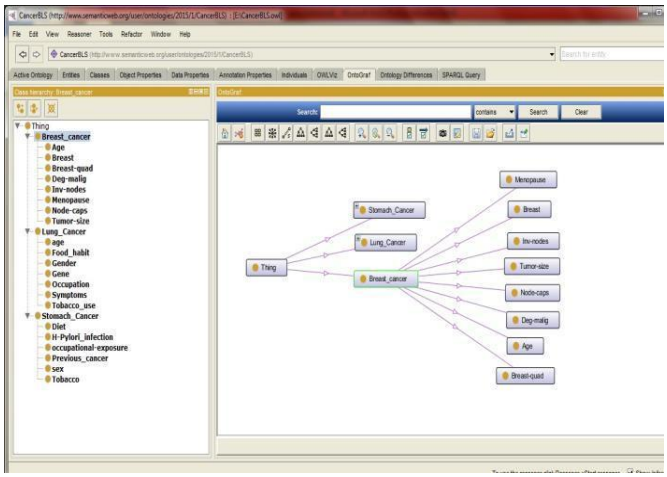


***Figure 2: Ontology graph for cancer disease.***

## VI. CONCLUSION

The proposed ontology-based system that provided an explicable and organized solution to capture knowledge regarding cancer patients‟ characteristics and then attribute based encryption algorithm addressed the security challenge of healthcare patients‟ knowledge while providing a framework for collaborative sharing and knowledge acquisition among the patients and clinicians.

## VII. REFERENCES

[1] http://globocan.iarc.fr/Pages/DataSource_and_methods.aspx.
[2] Furkh Zeshan, Radziah Mohamad, “Medical Ontology in the Dynamic Healthcare Environment,” Procedia Computer Science 10 (2012) pp. 340 – 348.

[3] A. Alesanco, J. García, N. Lasierra, F. Roldán, "Towards improving usage and management of supplies in healthcare: An ontology-based solution for sharing knowledge," Expert Systems with Applications 41 (2014) pp. 6261– 6273.

[4] Argyroula Christopoulou, Christos Skourlas, Petros Belsis, "Sharing Knowledge and Integrated Information in Therapeutic Radiological Physics," Procedia - Social and Behavioral Sciences 147 (2014) pp. 313 – 320.

[5] Aida Valls, David Sánchez, Karina Gibert, Montserrat Batet, "Using ontologies for structuring organizational knowledge in Home Care assistance," international journal of medical informatics 7 9 ( 2 0 1 0 ) pp. 370–387.

[6] Stephen J.H. Yang, Irene Y.L. Chen "A social network-based system for supporting interactive collaboration in knowledge sharing over peer-to-peer network," Int. J. Human-Computer Studies 66 (2008) pp. 36–50.

[7] Chuen Tse Kuah, Kuan Yew Wonga, Manoj Kumar Tiwari "Knowledge sharing assessment: An Ant Colony System based Data Envelopment Analysis approach," Expert Systems with Applications 40 (2013) pp. 3137– 3144.

[8] Amir Zidi, Amna Bouhana, Mourad Abed, Afef Fekih "An ontology-based personalized retrieval model using case base reasoning," Procedia Computer Science 35 (2014) pp. 213 – 222.

[9] Lifei Wei , Haojin Zhu , Zhenfu Cao, Xiaolei Dong , Weiwei Jia , Yunlu Chen , Athanasios V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Information Sciences 258 (2014) pp. 371– 386.

[10] Benjamin Fabian , Tatiana Ermakova , Philipp Junghanns "Collaborative and secure sharing of healthcare data in multi-clouds" Information systems, Elsevier (2014) in press.

[11] http://en.wikipedia.org/wiki/Web_Ontology_Language.

[12] http://www.w3schools.com/webservices/ws_rdf_owl.asp.

[13] UCI Machine Learning Repository. http://www.ics.uci.edu/mlearn/MLRepository.html for breast cancer dataset.

[14] http://www.protege.stanford.edu/protege.

[15] Yang, D.; Miao, R.; Wu, H.; Zhou, Y.;, "Product configuration knowledge modeling using ontology web language," *Expert Systems with Applications*, vol. 36, no. 3, (2009) pp. 4399–4411.

[16] Sujan Perera, Cory Henson, Krishnaprasad Thirunarayan, Amit Sheth and Suhas Nair, " Semantics Driven Approach for Knowledge Acquisition From EMRs" IEEE Journal Of Biomedical And Health Informatics, , vol. 18, no. 2, (2014) pp. 515–524.