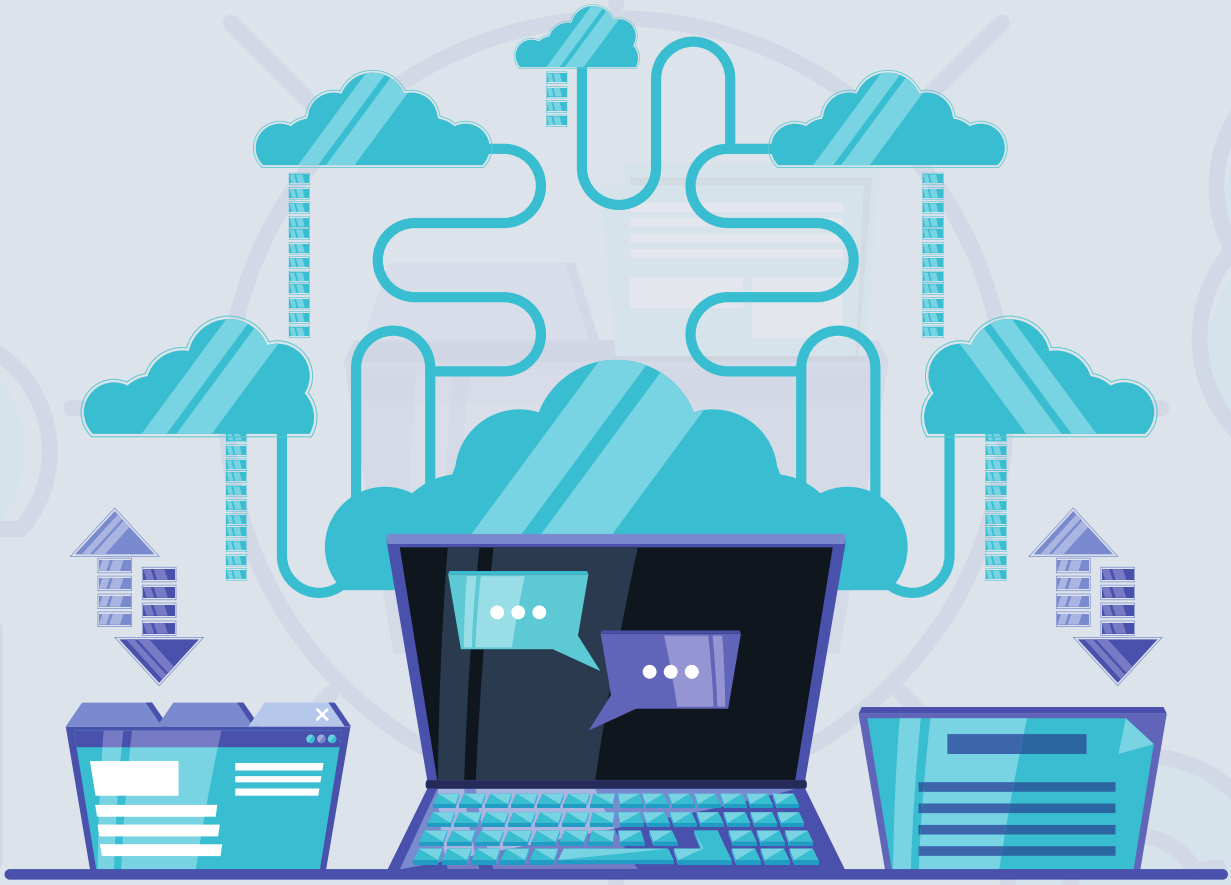
Onto ED: Ontology-Based Algorithm to Perform Encryption & Decryption in Multi-Tenant Cloud Environment

*Dimpy Jindal, **Barkha Bahl



Abstract **:**
Information is expanding day by day and it comes with irrelevance and lack of security. Also, it is mandatory to reduce time complexity by providing relevant results to users so that they can directly access the services on the cloud based on pay per usage policy. The paper proposes an ontology-based algorithm to perform encryption and decryption of input data in a multi-tenant cloud environment. It involves the classification of classes, properties, and instances of plain text by designing ontology related to a specific domain. The ontology is designed with the help of an ontology editor called Protégé and performs accessing of relevant data from cloud service providers on pay per usage policy.

Keywords : *Cloud computing, Multi-tenancy, Ontology, Algorithm, Encryption, and Decryption*

**Assistant Professor, Sirifort Institute of Management Studies, Delhi, India*
*** Director, Trinity Institute of Professional Studies, Delhi, India*

INTRODUCTION

Cloud computing has opened the doors to various researchers and businesses by offering several advantages including but not limited to huge storage, faster access, and easy availability of data (Krishnaraj N., et al 2021). It can be done by setting specific attributes based on regulation policies and guidelines of the Information Technology Act, of 2000 (Subedar Zuhi, et al 2020). For maintaining the encryption and decryption of data, the specified attributes must meet the constraints defined in the access policy (Lin R.,et al 2018, Rosalina,et al 2020). The data must be encrypted before sharing it to the cloud to maintain security in the system (Mohammed C. M., et al 2021). The manager behind the provision of various services to the users is the Cloud Service Provider (CSP). The input data/cipher text is produced by the data owner which is responsible for uploading text to the CSP. The required text is then decrypted and accessed by the user with the help of CSP. Each user is termed as a tenant and the process of multiple tenants sharing data is often termed as Multi-tenancy (Zulifqar Isma,et al 2021). In this, the shared data is not interacted with other tenants by providing a separate architecture framework on CSP (Wang S.,et al 2016). Multi-tenancy is performing encryption and decryption in an improved and efficient way. When a malicious user tries to maintain unauthorized access to the server, a cryptographic hash function gets activated followed by a password dialog box It is succeeded by a secure socket layer (SSL) to authenticate the login details of the user. The information is not shared with other tenants residing on CSP and the authenticated tenant can only decrypt the original message with the help of a secured algorithm. This is how the process of encryption and decryption works in a multitenant cloud environment (Wang S., et al 2016, Arshad Muhammad Junaid, et al ,2020).

1.1. SIGNIFICANCE OF THE STUDY

Information is expanding day by day and it comes with irrelevance and lack of security. Also,it is mandatory to reduce time complexity by providing relevant results to users so that they can directly access the services on the cloud based on pay per usage policy. Hence, this research work attempts to provide an efficient and reliable means of data access in a multi-tenant cloud environment.

The study aims to propose an algorithm to access data securely and reliably. It works in such a way that it creates an ontological database in the cloud. The database deals with the development of ontology, mapping of relational schemes into semantic schemes, and provision of services to the users on the cloud.

1.2. PROBLEM STATEMENT

Recent studies comprise various challenges like irrelevant results, complexity issues, lack of relationship between user requests and data attributes, etc. thereby affecting the end data retrieval results. The paper overcomes the aforementioned issues by proposing an algorithm based on semantic rule inferences and an ontological database.

1.3. MOTIVATION FOR RESEARCH

Traditional keyword-based searches from cloud centers lead to irrelevant and large numbers of results which increase complexity for the users and distinguishing relevant results from huge collections is a cumbersome task. To overcome this problem, the study aims to create and develop an ontological database in the cloud for performing encryption and decryption of data in an enhanced manner.

1.4. METHODOLOGY

The study performs doctrinal research by analyzing various research papers published in conferences and journals including but not limited to IEEE, Scopus, and other International journals.

1.5. PAPER ORGANIZATION

The given paper is organized into the following sections. Section 2 presents a brief literature review of the studies conducted in the context of encryption, decryption process in a multi-tenant cloud environment. Section 3 makes readers aware of the basic concept of ontology in the cloud. Section 4 describes the proposed algorithm based on semantics and ontological database and its implementation. Section 5 provides a conclusion and future scope followed by references.

ITERATURE REVIEW

A framework based on the cloud is described in (Li J., Z,et al 2018) that S.,et al 2020) Used a secured keyword search based on Bloom filter to enable ranking of results. It only retrieves relevant data from the user. (Kumar P.,et al 2020) made use of the ECC (Elliptic curve cryptography) algorithm for performing encryption of data and authentication of tenants. This method also protects from diverse attacks. (Yarava R. K., et al 2019) used the Diffie Hellman technique to perform key exchange in a cloud environment thus enhancing auditing performance and the key generated is also shared with the user. (Li J., et al 2018) suggested a method to overcome a load of complexity by includingpublic parameters for performing encryption followed by decryption of cipher text in a cloud environment. Cloud architecture was proposed by (Yu R., et al 2015) to incorporate virtual networks application in a cloud-based environment thereby focusing on management and security. In (Peng G., et al 2016), the estimation of the complexity of software in cloud architecture is computed using simulation based on quality and quantity parameters. This is done by using a radial-based neural network by constructing a mathematical model based on the priority of load balance by tenants.

Table 1: An Overview of Related Works

Author/Citations	Technique used	Pros	Cons
Chang et. al	Firewall management	Robust and multi-layered	Unable to recognize threats on time
Ali et.al	Keyword filtering technique	Provides relevant data to the user based on synonyms	No concept of ontology is being used
Kumar et.al	Elliptic curve cryptography	Protects data from malicious attacks	Does not store keys in the database generated by the user
Singh et.al	Diffie Hellman exchange	Performs encryption by sharing keys with users	Violates the concept of multi-tenancy by sharing keys among users without creating a separate base for each user.
Zhang et.al	Parameter based exchange	Performs encryption and decryption of data in response to time complexity.	Data is accessed from relational schema which increases the computation time of the retrieval process.
Yu et.al	Virtual networks	Focuses on the security of data by making use of VPN and firewall systems.	Complex and costly process
Peng et.al	Neural networks	Performs computation of load balancing on the cloud environment	No specific parameters and measures

ONTOLOGY IN CLOUD

Ontology is treated as the formal ,explicit specification of a shared conceptualization (Gartner, et al 2012). Besides its formal nature, philosophical aspects, and handling of real-world scenarios, it also acts as a medium for linking humans and machines. Ontology in itself is a vast research area that includes mapping, merging, extraction, moving, and evaluation of ontologies.

Ontology evaluation approaches are classified into the following categories (Kalyan CC, et al 2013).

- Based on comparing ontologies
- Based on the usage and application of ontologies
- Based on the set of documents related to a domain ontology
- Based on human evaluation to meet ontology requirements and compatibilities.

PROPOSED WORK

In the proposed system, data is made to be secured by performing encryption-decryption by taking ontology as the backend in a cloud database. The suitable ontology is designed with the help of an ontology editor based on the domain of input data. Then, it is mapped from the relational schema into the ontology database to generate meaningful results. Using ontology as a backend leads to the retrieval of efficient search results for the user. When a tenant wants to access data on a cloud database, the request is sent to the cloud service provider (CSP). It requires the authentication of a tenant by entering login details in the system. Each tenant is given a hash key function to ensure the integrity of data or plain text. The plain text is converted to cipher text by encryption and decryption using a secure key transfer.

Algorithm

Step 1: Initialization

Ip= Input data
Ct= cipher text
Ui= user requests to access data by sending key requests.
Csp= cloud service provider
Ul= user login details
Pk1= Public key for encryption
Pk2= Private Key for decryption
Step 2: Encryption process (Ep)
Hk= hash key function
Pt to Ct= Plain text is converted to cipher text
Ep= (Pk1 * Pk2) + Ip*Hk
Step 3: Creation of ontological database Ip is converted from a relational schema to an ontological database by designing ontology with the help of editors like PROTÉGÉ. A sample of the designed ontology is shown in Figure 2.

Step 4: Defining classes, properties, and instances related to the data domain that needs to be accessed from the cloud. It includes coding in Java which is used to show defined classes, subclasses, and instances.

Step 5: Creation of an ontological grid to access data from the cloud in a hierarchical form. It is shown in Fig 3

Step 6: Decryption process (Dp)
Ct to Ip for both the keys
Dp= (Pk1 * Pk2)

Step 7: Integration of ontological database into the cloud

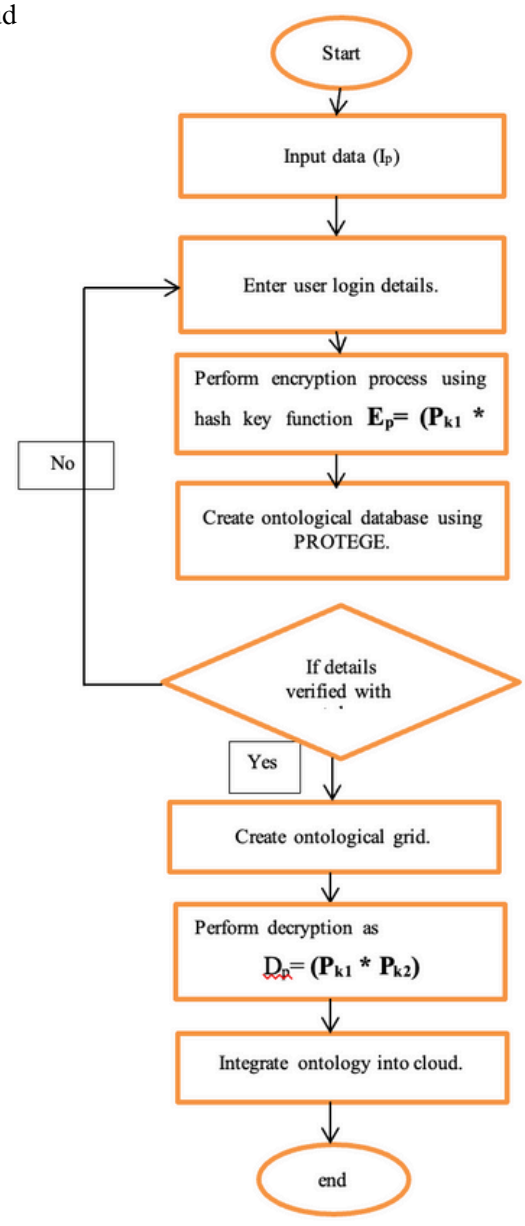


Figure 1: Flowchart of the proposed Onto ED algorithm

4.1. Snippet Codes & Implementation

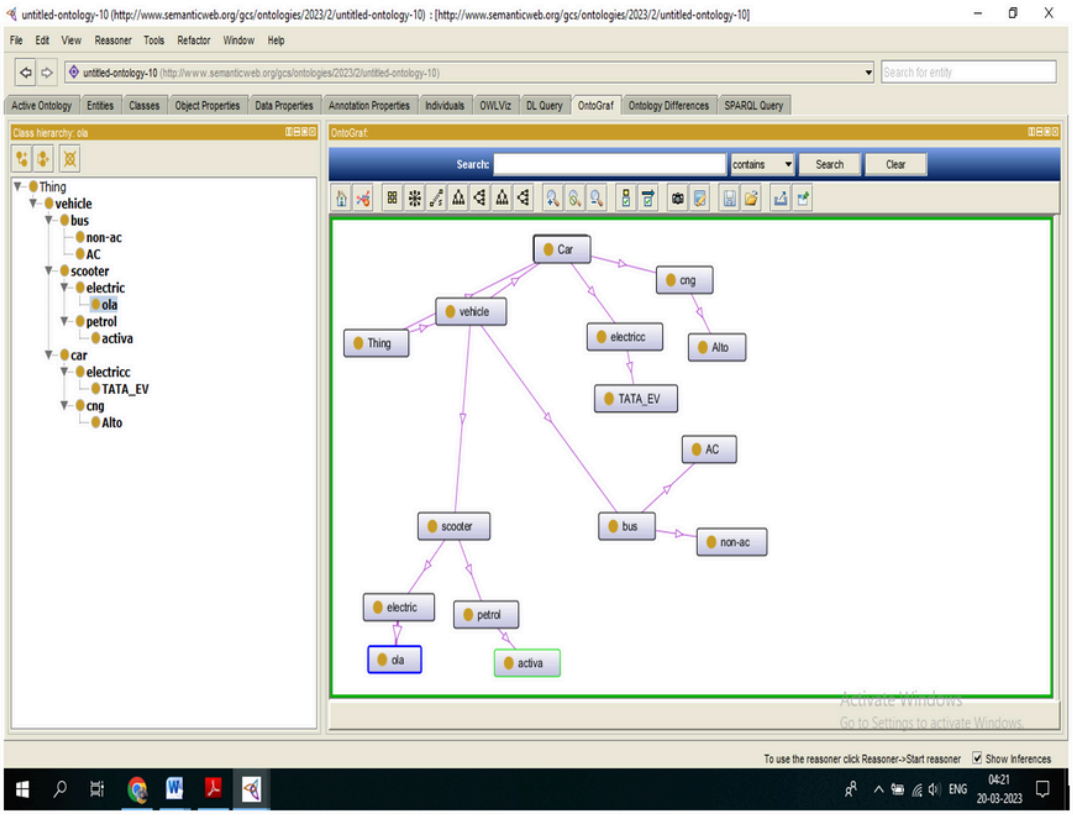


Figure 2: Ontology designed in PROTEGE to be stored as backend in a cloud

In figure 2, it is evident that relationship between classes-subclasses and their instances are maintained.

Consider car as class which has sub classes electric and cng. In response to this, Alto and TATA_EV are its instances.

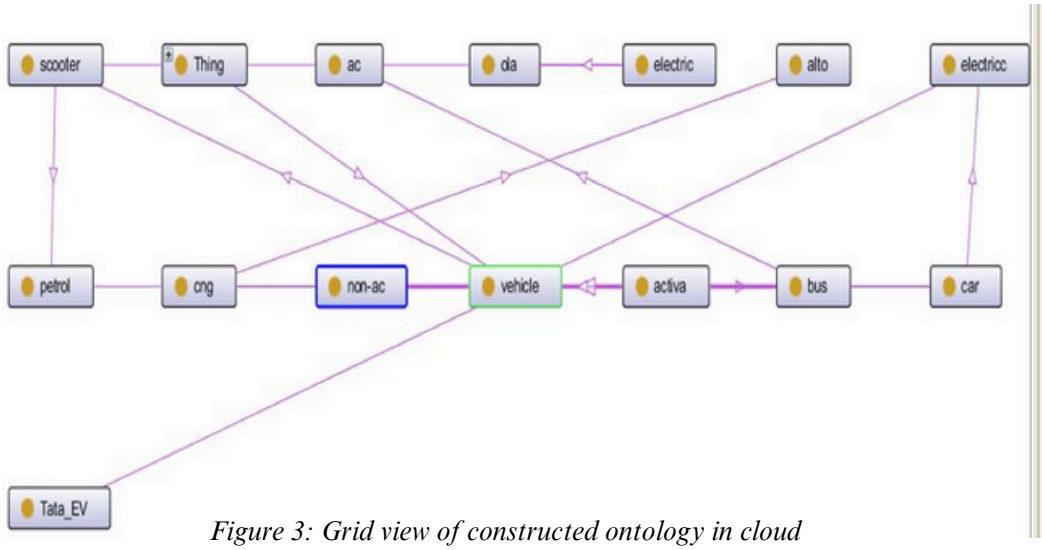


Figure 3: Grid view of constructed ontology in cloud

The above-designed ontology in figure 3 utilizes a snippet coded in Java that is used to perform the decryption of text by combining classes, properties, and instances from an ontological database.

In this figure, the classes and sub-classes are formed in grids leading to cluster partitions in cloud environment. It leads to more scalability and easy retrieval of information from the cloud.

4.2. Coding involved in designing an ontology

4.2.1. Extending bus class

```
package vehicle;
import java. util.Collection;
import
org.protege.owl.codegeneration.WrappedIndividual;
import
org.semanticweb.owlapi.model.OWLNamedIndividu
al;
import
org.semanticweb.owlapi.model.
OWLOntology;
public interface Ac extends Bus
{OWLNamedIndividual getOwlIndividual();
OWLOntology getOwlOntology();
void delete(); }
```

4.2.2 Extending super class Vehicle

```
package vehicle;
import java.util.Collection;
import
org.protege.owl.codegeneration.WrappedIndividual;
import
org.semanticweb.owlapi.model.OWLNamedIndividu
al;
import
org.semanticweb.owlapi.model.OWLOntology;
public interface Vehicle extends WrappedIndividual {
OWLNamedIndividual getOwlIndividual();
OWLOntology getOwlOntology();
 void delete();}
```

4.2.3. Snippet to integrate data into the cloud

```
class Bus extends Vehicle
{ public Bus(Agent a) { super(vehicle);}
 public void action()
{ ACLMessage msg = receive();
 if (msg == null) { block(); return; }
 try {Object content = msg.getContentObject();
 switch (msg.getPerformative()) {
 case (ACLMessage.REQUEST):
 if (action instanceof CreateAccount)
  addBehaviour(new HandleCreateAccount(myAgent,
msg));
else if (content instanceof MakeOperation)
    addBehaviour(new HandleOperation(myAgent,
msg));}}
class Handle Operation extends OneShotBehaviour {
ACLMessage request;
public HandleOperation(Agent a, ACLMessage
request) { super(vehicle);
 this.request = request }
 public void action() {
 try {
 Operation op = (Operation)
 request.getContentObject();
 ACLMessage reply = request.createReply();
 // Process the operation
 Object result = processOperation(op);}
 catch (Exception ex) { ex.printStackTrace(); }
}
}
```

4.3. Validation of the proposed approach

The proposed ontological based framework is validated by using dataset other than vehicle dataset to show the transparency of cloud environment and its functioning. Keeping this in mind, the paper takes dataset related to BREAST CANCER WISCONSIN DATASET into consideration (Bennett K. P. et al, 1992). It is taken from Kaggle. The dataset consists of attributes namely clump thickness, uniformity of cell size, uniformity of cell shape, marginal adhesion, bare nuclei and mitosis. The above mentioned algorithm is applied on dataset to perform encryption and decryption in cloud. It is done in simulation platform named ANEKA and WEKA cloud platform.

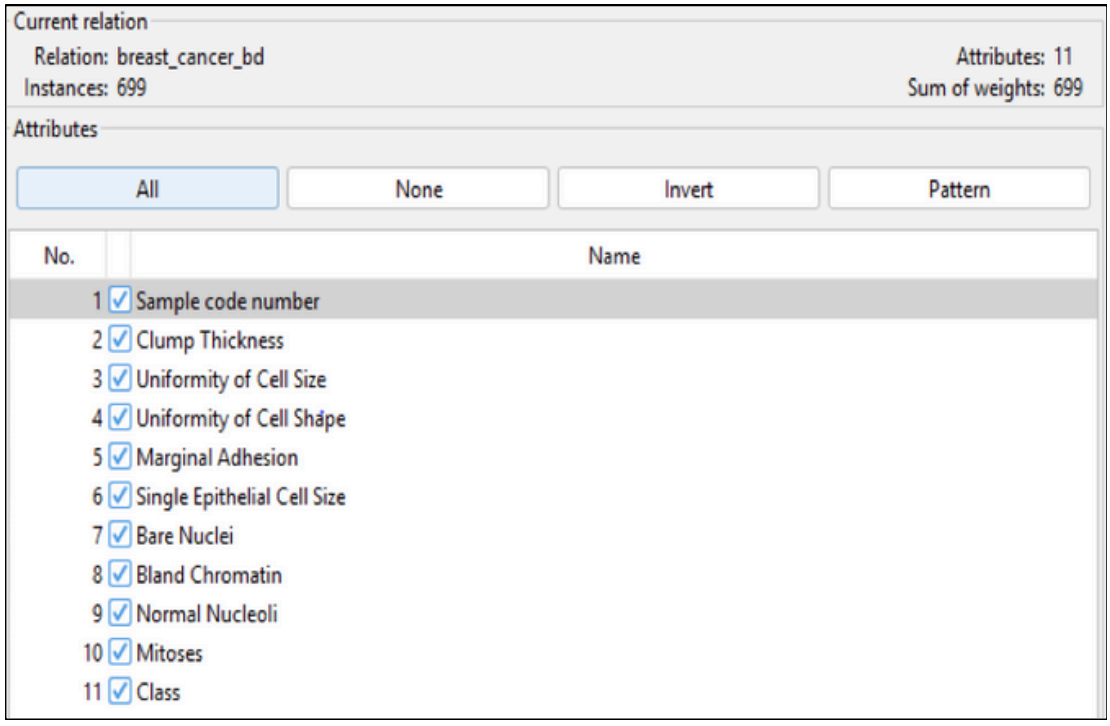


Figure 4 : Attributes of breast cancer dataset (Bennett K. P. et al, 1992)

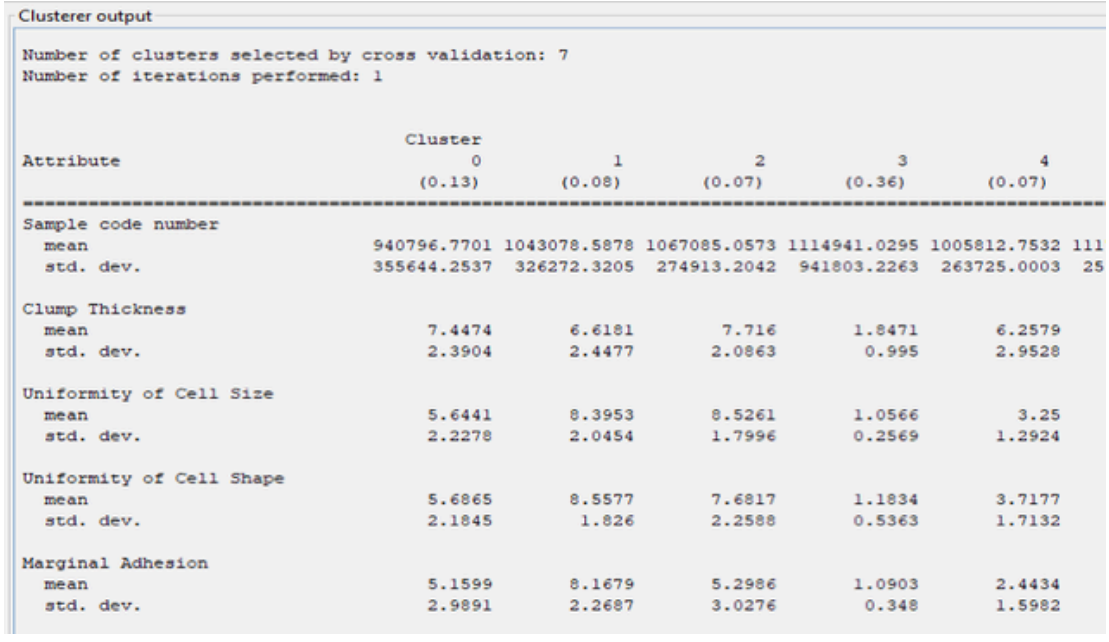


Figure 5 : Clustering of dataset and computing mean+ standard deviation of encrypted data in cloud environment

In figure 5, it is seen that the data undergoes encryption using proposed algorithm followed by calculation of mean and standard deviation of attributes to validate the performance of the proposed system.

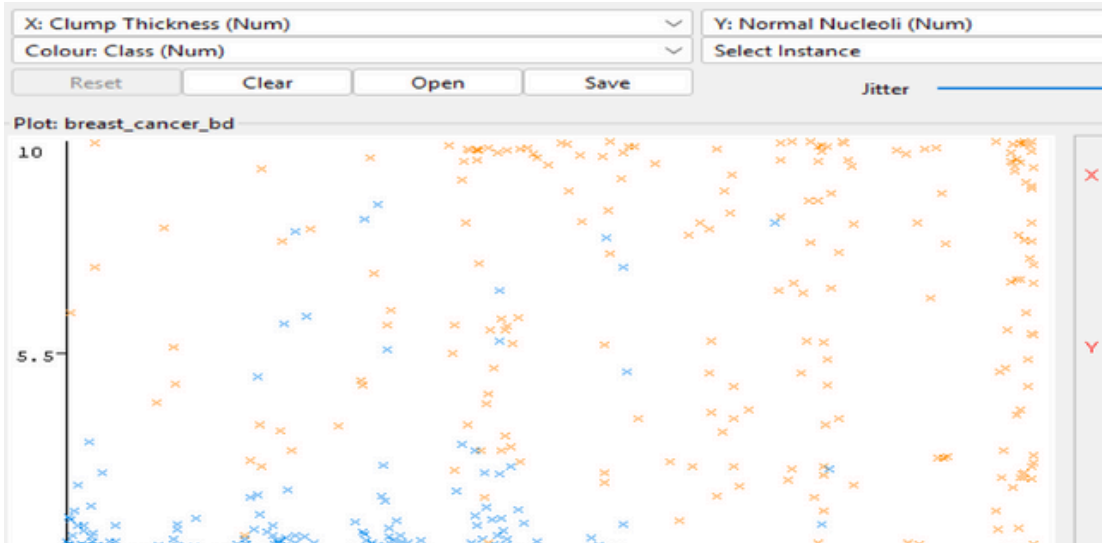


Figure 6 : Representation of attributes namely clump thickness (x-axis) and nuclei (y-axis) with the help of WEKA and transferring these values to cloud using ANEKA

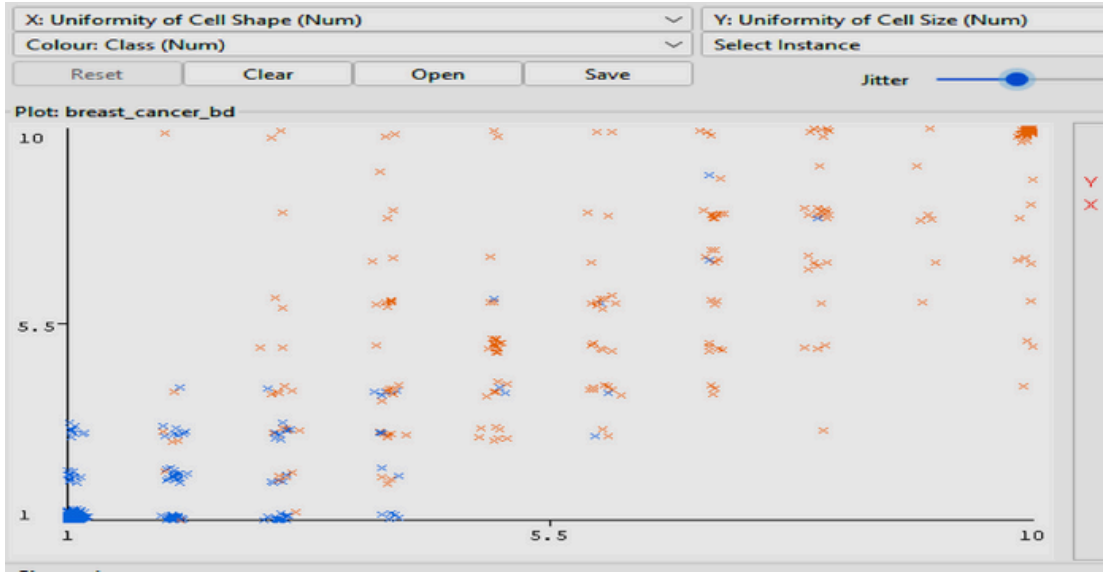


Figure 7: Representation of attributes namely uniformity of cell shape (x-axis) and uniformity of cell size (y-axis) with the help of WEKA and transferring these values to cloud using ANEKA

Our proposed approach is compared with the existing approach given in (Ali F. S.,et al 2020) based on computation time and accuracy. The proposed approach takes less computation time to process data

The proposed approach takes less computation time to process data and perform encryption-decryption as compared to the existing approach. It is shown in figure 8.

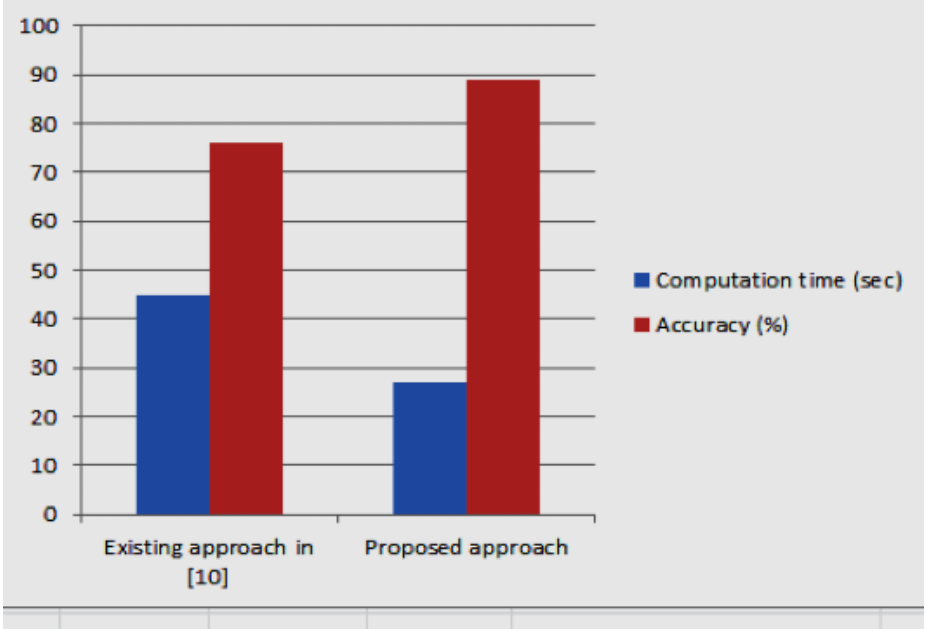


Figure 8: Comparison of proposed approach and existing approach

CONCLUSION AND FUTURE SCOPE

The following paper overcomes the complexity issues, and irrelevance of search results by proposing an ontology-based algorithm to access secured data in a multi-tenant cloud environment. It is done by performing encryption and decryption with the help of hash functions and keys to maintain the relationship between the input data and cipher text. It is done by interacting with multiple tenants by designing ontology with the help of an ontology editor named PROTEGE.

The ontology designed is stored in a cloud database in respective layers of SaaS and tenants are made to access classes and attributes of ontology based on Pay per usage policy.

As a future scope, ontology can be designed using other editors also, and the results are filtered with the help of collaboration filtering. It is one of the recommended steps to enhance ontology in the SaaS layer of the cloud.

REFERENCES

- *Ali F. S., H. N. Saad, Sarhan F. H., and Naaeem B., (2020) "Enhance manet usability for encrypted data retrieval from cloud computing," Indonesian Journal of Electrical Engineering and Computer Science, vol. 18, pp. 64-74.*
- *Arshad Muhammad Junaid, Umair Muhammad, Munawar Saima, Naveed Nasir, Naeem Humaira, (2020) "Improving Cloud Data Encryption Using Customized Genetic Algorithm", International Journal of Intelligent Systems and Applications (IJISA), Vol.12, No.6, pp.46-63. DOI:10.5815/ijisa.2020.06.04*
- *Bennett K. P. and Mangasarian O. L. (1992) "Robust Linear Programming Discrimination of Two Linearly Inseparable Sets", Optimization Methods and Software 1, 23-34.*
- *Chang V., Kuo Y.-H., and Ramachandran M., (2016) "Cloud computing adoption framework: A security framework for business clouds," Future Generation Computer Systems, vol. 57, pp. 24-41.*
- *Gartner, Dhoedt Bart and Demeester Piet, (2012) "Cloud-Based Desktop Services for Thin Clients", IEEE Computer Society, Nov/December 2012, pp 60-67*
- *Kalyan CC, Lokesh, (2013) "Security Techniques for multi tenancy applications in cloud", IJCSMC, Vol2 Issue 8, pp 248-251*
- *Krishnaraj N., Elhoseny M., Lydia E. L., Shankar K., and ALDabbas O., (2021) "An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in a cloud environment," Software: Practice and Experience, vol. 51, pp. 489-502.*
- *Kumar P. and Bhatt A. K., (2020) "Enhancing multi-tenancy security in the cloud computing using hybrid ECC-based data encryption approach," IET Communications, vol. 14, pp. 3212-3222.*
- *Li J., Zhang Y., Chen X., and Xiang Y., (2018) "Secure attribute-based data sharing for resource-limited users in cloud computing," Computers & Security, vol. 72, pp. 1-12.*
- *Lin R., Wu B., and Su Y., (2018) "An adaptive weighted Pearson similarity measurement method for load curve clustering," Energies, vol. 11, p. 2466.*
- *Mohammed C. M. and Zebaree S. R., (2021) "Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review," International Journal of Science and Business, vol. 5, pp. 17-30.*
- *Peng G., Wang H., Dong J., and Zhang H., (2016) "Knowledge-based resource allocation for collaborative simulation development in a multi-tenant cloud computing environment," IEEE Transactions on Services Computing, vol. 11, pp. 306-317.*
- *Rosalina, Hadisukmana Nur, (2020) "An Approach of Securing Data using Combined Cryptography and Steganography", International Journal of Mathematical Sciences and Computing (IJMSC), Vol.6, No.1, pp.1-9. DOI:10.5815/ijmsc.2020.01.01*
- *Singh Gagandeep, Jain Vishal, (2012) "Information Retrieval (IR) through Semantic Web (SW): An Overview", "In proceedings of CONFLUENCE 2012- The Next Generation Information Technology Summit at Amity School of Engineering and Technology", September, pp 23-27.*
- *Subedar Zuhi, Araballi Ashwini. (2020) "Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication", International Journal of Mathematical Sciences and Computing (IJMSC), Vol.6, No.4, pp.35-41. DOI:10.5815/ijMSC.2020.04.04*
- *Wang S., Zhou J., Liu J. K., Yu J., Chen J., and Xie J., (2016) "An efficient file hierarchy attribute-based encryption scheme in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, pp. 1265-1277.*
- *Yadav U., Singh Gagandeep, Duhan N., Jain V., (2016) "Ontology Engineering and Development Aspects: A Survey", IJEME, MECS Hong Kong, 3, 9-19.*
- *Yarava R. K. and Singh R. P., (2019) "Efficient and Secure Cloud Storage Auditing Based on the Diffie-Hellman Key Exchange," International Journal of Intelligent Engineering and Systems, vol. 12, pp. 50-58.*
- *Yu R., Xue G., Kilari V. T., and Zhang X., (2015) "Network function virtualization in the multi-tenant cloud," IEEE Network, vol. 29, pp. 42-47.*
- *Zulifqar Isma, Anayat Sadia, Khara Imtiaz, (2021) "A Review of Data Security Challenges and their Solutions in Cloud Computing", International Journal of Information Engineering and Electronic Business (IJIEEB), Vol.13, No.3, pp. 30-38. DOI:10.5815/ijieeb.2021.03.04*