Turkish Journal of Physiotherapy and Rehabilitation**; 32(2)**
ISSN 2651-4451 | **e-ISSN** 2651-446X

Privacy Protection in Cloud Computing

Sri lakshmi Medaboina[1],Dr.Moulana Mohammed[2]
[1]M. Tech Student, Department of CSE (Cyber Security and digital Forensics), Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India, medaboinasrilakshmi@gmail.com
[2]Associate Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India, moulana@kluniversity.in

ABSTRACT

Cloud computing is appearing like a prevalent data interactive paradigm to appreciate users data remotely stored in an internetcloud server.Cloud services supplybetterbenifits for the users to like the on-request cloud applications without thinking about the neighborhood foundation impediments. During the information getting to,different users areadditionally in a very collaborative relationship, and thus information sharing gets huge torealize productive benefits. The previous security methods-
mainly concentrateon theauthentication tounderstandthatauser'sprivativedata cannotbe unauthoriz edaccessed,butneglect a inconspicuous protection issue during a client moving the cloud worker to look for different clients for information sharing. The tested admittance demand itself may uncover the user's privacy despite whetheror not it can obtain the information access permissions. Previous System does not have the option of granting/revoking data access.In this paper, we proposedthe safedevice and informationholder can decide the user can use the system or not.

Keywords: cloud computing, authentication, privacy,users.

I. INTRODUCTION

The word cloud mentionto a network or the web. it's an innovation that utilizes isolated servers on the web to store, manage, and access knowledge on-line instead of native drives. the information will be something like files, images, documents, audio, video, and more[1].

There was the subsequent operations that we are able to do exploitation cloud computing:
o Developing new applications and services
o capacity, support, and retaking of information
o Hosting blogs and websites
o Delivery of code on demand
o Analysis of information
o Streaming videos and audio[1]

1.1.Types of Clouds

There was four totally different cloud models that you just will subscribe per business wants. Following square measure the various sorts of Clouds[2]:

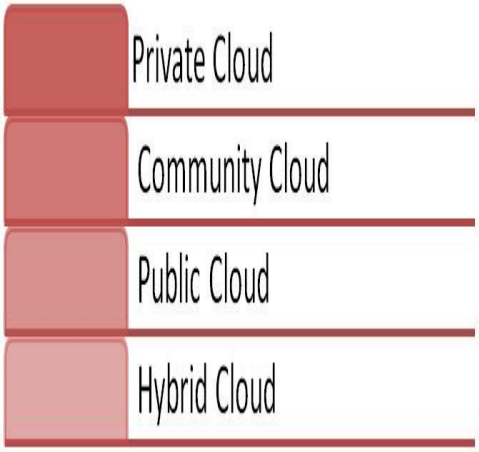

Figure-1:Types of Clouds

1. personal Cloud: Here, computing resources area unit deployed for one specific organization. This technique is a lot of used for intra-business interactions. wherever the computing resources are often ruled, owned and operated by identical organization.
2. Community Cloud: Here, computing resources was provided for a community and organizations.
3. Public Cloud: sort|this sort|this kind} of cloud is employed sometimes for B2C (Business to Consumer) type interactions. Here the computing resource is owned , ruled and operated by government, an educational or business concern.
4. Hybrid Cloud: this kind of cloud are often used for each style of interactions - B2B (Business to Business) or B2C (Business to Consumer). This preparation technique is named hybrid cloud because the computing resources square measure sure along by totally different clouds.[2]

Over the last few years, cloud computing has quicklyappear as a widely believed computing model built around several concepts similar to on-demand computing resources, elastic scaling, elimination of up-front capital and operational expenses, and establishing a pay-as-you-go business model for computing and data technology services [4].

Cloud computing could be a promising info technology introducefor all enterprises and customers. It launches engaging information storage and interactive paradigm with obvious benefits, together with on-demand self-services, present network access, and site unconventional resource pooling [5].

Distributed computing, presence a few assets like IaaS(Infrastructure as a service),PaaS (Platform as an administration) ,SaaS (Software as an administration), is predominantly partitioned into a few organization models like Public cloud, private cloud, mixture cloud etc. based on manyformation types security level varies[3].

- **IaaS(Infrastructure as a service)-**IaaS suppliers provide the cloud servers and those associated resources through a dashboard and/or API. IaaS purchasers have straightgain to their servers and capacity, accessing to a way higher measurability. Users of IaaS will source and build a “virtual information center” within the cloud and approach to several of a similar technologies and resource capabilities of a conventional information center while not having to speculate in capability designing or the actual support and the executives of it[3].
- **PaaS(Platform as a service)-** PaaS provides a platform on that software package will be developed and deployed. PaaS suppliers offer purchasers such associate atmosphere within which the OS and server software package, also basic worker equipment and organization infrastructure area unit taken care of, effort users unengaged to concentrate on the business aspect of measurability, and also the application improvement of their product or service[3].

- **SaaS(Software as a service) –** In thistype, suppliers offer the purpose of access to software system running on servers. SaaS is most confidential type of cloud service for customers. It moves the task of managing software system and its preparation to third-party services. Salesforce, Google Apps, Dropbox are the some common SaaS model.
-

Figure-1 shows the different cloud services diagrammatically[10].

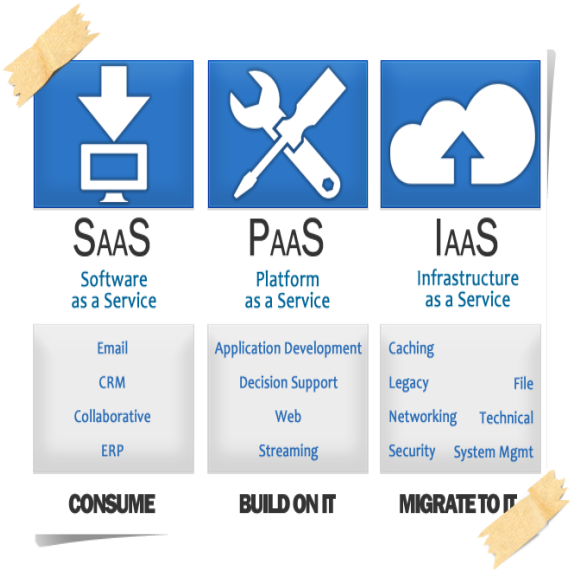

Figure-2:different types of cloud services

Data integrity issues within the cloud differ from those in traditional database systems. Cloud users are better discussed about whether data center owners will misuse the system by arbitarly using private datasets or releasing sensitive data to a 3rd party without authorization[7].

In the cloud conditions, an affordable security protocolshould accomplish the subsequent uses. 1) Authentication: a legal user will access its own knowledge fields, just the approved partial or entire information fields are often known by the legal user, and any cast or tampered information fields cannot deceive the legal user[8]. 2) information associateonymity: any inapplicable entity cannot acknowledge the changed information and communication state even it intercepts the changed messages via an open channel. 3)User privacy: any inapplicable entity cannot understand or guess a user's access need, that represents a client's advantage in another client's approved information fields. If and given that the each users have mutual interests in every other's approved information fields, the cloud server can inform the 2 users to understand the access permission sharing. 4) Forward security: any opponent cannot correlate more than one correspondence meetings to infer the previous interrogations per the presently captured messages[5].

II. Existing system

Data security/privacy is one ofThemajor concerns in the adoption of cloud computing[9].
However, most previous researches concentrate on the authentication to understand that just a legal user will access its licensed information, that ignores the case that completely different users might want to access and share every other's licensed data fields to achieve beneficial advantages. once a user challenges the cloud worker to demand various clients forinformation sharing, the access request itself might reveal the user's privacy despite of regardless of whether.it will be get the knowledge access permissions. during this work, we tend to aim to handle a user's sensitive access need equal privacy throughout information sharing within the cloud environments, and it's important to model a humanistic security theme to at the same time attain information access management, access authority

sharing, and privacy preservation[11].the most disadvantage in previous system is that the Previous System doesn't have the choice of granting/revoking information access.

III. Proposed system:

Here we proposed the made sure about framework and information proprietor can decide if the client can utilize the framework or not.In this model, protection is refined by encrypting the information it can prevent the un authorized access.We are going to raise the security level of the data owner also, the privacy of the data by providing access to users.

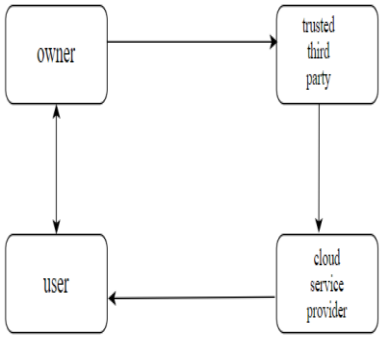

Figure-3:propoed system architecture

Modules in proposed system are

- Owner
- User
- Access Control
- Cloud Service Provider
- Encryption & Decryption
- File Download
- Trusted Third Party

Owner Registration:
during this section a owner must transfer its files into cloud server, he/she must register 1st. Then solely he/she may be able to have a go at it. For that he must fill the main points within the registration page. These details be maintained during a information.

Owner Login:
during this section,any of the beyond mentioned person need to login,they ought to login by giving their emailid and password .

User Registration:
At this section if a user needs to access the information that is keep during a cloud, he/she ought to register their details 1st. These details be maintained in information.

User Login:
If the user is a licensed user, he/she will transfer the file by utilize file id that has been keep by information owner once it had been uploading[6].

Access Control:

Owner will allow access or deny access for accessing the information. therefore users will able to access his/her account by the corresponding information owner. If owner doesn't permit, user can't able to get the information.

Encryption & Decryption:

Here i am utilizing this aes_encrypt & aes_decrypt for encoding and decoding. The file we've uploaded that must be in encrypted type and decode it

Code for encryption

```
<%
string date=(string)session.getAttribute("date);
string fkey=(string)session.getAttribute("fkey);
string fid=(string)session.getAttribute("fid);
string fname=(string)session.getAttribute("fname");
string fsize=null;
FileInputSteam fis;
preparedStatement psmt1=null;
try
{
Connection conn=databasecon.getconnection();
psmt1=con.preparestatement("insert into file values(?,?,?,?,AES_ENCRYPT(?,'key'),?)");
File f= new File(saveFile);
psmt1.setString(1,fid);
psmt1.setString(2,fname);
psmt1.setString(3,fkey);
psmt1.setString(4,date);
fis=new FileInputStream(f);
psmt1.setBinaryStreamStream(5,(Inputstream)fis,(int)(f.length()));
double bytes = file.length();
fsize=Double.toString(bytes);
psmt1.setString(6,fsize);
psmt1.executeupdate();
response.sendRedirect("admin_fileupload.jsp?message=success);
}
catch(Exception ex)
{
out.println("error in connection : "+ex);
}
}
%>
```

Fig-3 shows the encrypted form of file which was uploaded by owner.

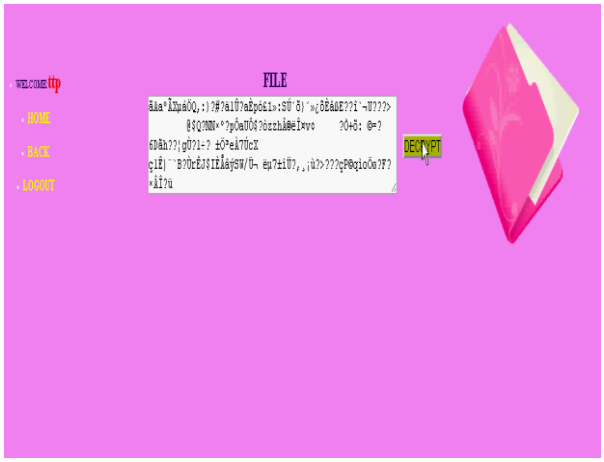

Figure-4: Eccryption form of uploadedfile

Code for decryption:

```
<%
string name=(string)session.getAttribute("name");
string fid=(string)session.getAttribute("fid);
string fsize=null;
try
{
string t= null;
connection con=databasecon.getconnection();
preparedstatement ps=con.preparestatement("select AES_DECRYPT(file,'key'),fsize from file where fid=' "+fid+"'");
resultset rs= ps.executequery();
while(rs.next())
{
Blob file = rs.getBlob("AES_DECRYPT(file,'key')");
byte [] b = file.getBytes(1,(int)file.length());
t=new string(b);
session.setAttribute("t",t);
fsize=rs.getString("fsize");
}
}
catch(Exception e1)
{
out.println("error in connection : "+ex);
}
%>
```

Fig-4 shows the decryption form of file which was decrypted by authorized user.

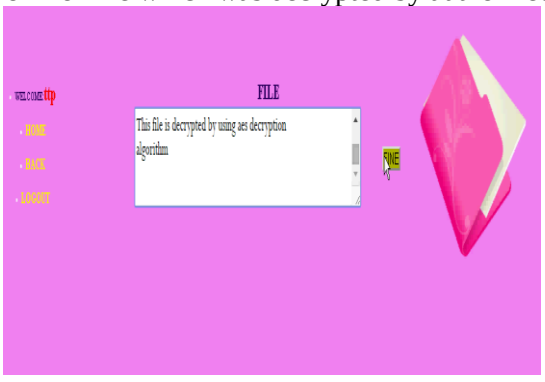

Figure-5:decryption form of file

File Upload:
during this element Owner transfer the file(along with meta data) into information, with the use of this information and its contents, the top user must transfer the file. The uploaded file was in encrypted type, solely registered user will decode it.

File Download:
The licensed users will transfer the file from cloud info.

Cloud Service supplier Registration:
In this section, if a cloud service provider(maintainer of cloud) needs to try and do some cloud supply , they ought to register 1st.

Cloud Service supplier Login:
when Cloud supplier gets logged in, He/ {she will|she will|she will be able to} see Cloud supplier can read the files uploaded by their purchasers. additionally transfer this document into independent Cloud data.

TTP (TRUSTED THIRD PARTY) LOGIN:
In this section TTP has monitors file house owners file by confirming the information owner's file and hold on the data in a info .Also ttp checks the CSP(CLOUD SERVICE PROVIDER),and determine whether or not the csp is allowed one or not.

IV. Conclusion

In this work, we've got known a replacement privacy challenge throughout information accessing within the cloud computing to realize privacy-preserving access authority sharing. Authentication is established to confirm information confidentiality and knowledge integrity. information obscurity is achieved since the wrapped values was changed throughout transmission. User privacy is expanded by unknown access demands to privately inform the cloud server regarding the users' access needs. Forward security is refined by the meeting identifiers to forestall the meeting relationship. It shows that the planned theme is probably applied for increased privacy preservation in cloud applications.

REFERENCES

1. cloudcomputingtutorial.(2018).javatpoint.retrievedfromhttps://www.javatpoint.com/cloudcomputing-tutorial
2. cloudcomputingforbiginers.(2019).Guru99retrievedfromhttps://www.guru99.com/cloudcomputing-for-beginners.html
3. Oberoi,R., & Dey, S. (2017). Survey of Security Issues in Cloud based E-Commerce. International Journal, 7(5).
4. Mishra, A., Jain, R., & Durresi, A. (2012). Cloud computing: networking and communication challenges. IEEE Communications Magazine, 50(9), 24-25.
5. Badadali, S. P., & Sujith, M. A.(2015). An Efficient Authentication Protocol for the Privacy Issues in the Cloud Storage based on Shared Access Authority Mechanism.
6. Prashanthi, K., Sangamithirai, P., & Pothumani, S. (2015). Secured Data on Cloud Environment by SAPA Protocol with Auto-renewal. Compusoft, 4(4), 1619.
7. Hwang, K., & Li, D. (2010). Trusted cloud computing with secure resources and datacoloring. IEEEInternetComputing, 14(5),14-22.
8. Bagade,R.,&Barde,C.R.(2015).Multi-userDataSharingAuthenticationProtocolforCloudComputingwithSeclusion.
9. Liu,C.,Chen,J., Yang, L. T., Zhang, X., Yang, C., Ranjan, R., & Kotagiri, R. (2013). Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates. IEEE Transactions on Parallel and Distributed Systems, 25(9), 2234-2244.
10. Sharma, M., Husain, S., & Zain, H. (2017). Cloud Computing Architecture& Services. IOSR J. Comput. Eng, 19(02), 13-18.
11. Xiong, H., Zhang, H., & Sun, J. (2018). Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing. IEEE Systems Journal, 13(3), 2739-2750.