|| Volume 6 || Issue 3 || March 2021 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

PRIVACY PROTECTED OWNER CENTRIC CLOUD DATA CONTROLLABILITY WITH SUPERVISED ACCESS POLICY

K.Soni[1], Dr. Shaik Shavali[2]

Research Scholar, Dept. of Computer Science & Engineering, LIET, Hyderabad[1]

Professor, HOD, Dept. of Computer Science & Engineering, LIET, Hyderabad[2]

-- ***---

Abstract: - Privacy protection is a crucial attribute to be focused on in Cloud computing great beneficial factor aside to facilitate reliability and trustability over cloud data access mechanisms. Data resource of a cloud data owner is to be secured and safeguarded effectively by using appropriate encryption strategy which in turn may not have control over the resource access policies. Cloud Service Provider of course has control over cloud data as a whole but cannot provide the data owner personalized access control policy leads to lag over high standard of cloud controllability. Data resource utilization by data users is been controlled by cloud Service Provider where-in all the data transactions made by data users don't let data owners have control over their specific data. There is a chance of lack of security when an intruder tries to access the cloud data a huge number of times to raise financial denial of sustainability threats in such that cloud data of specific data owner will be accessed improperly. Not only that data owner lacks data privacy but also disturbs the resource utilization access policies between cloud accountant and data owner. Putting data privacy of data owner which could be done by a high secured Cipher-Text policy-based encryption a side we should emphasize on resource access controllability to cloud data owner in such that financial terms between data owner and Cloud Service Provider will be maintained in healthy environments. In this proposed approach we emphasize fine-grained data access control towards owner-specific access policy strategy along with the privacy preservation of data owner's data with a sophisticated cipher-text policy-based encryption mechanism. In this data on a specific axis control strategy, we emphasize crucial operations like the search of cloud data, download activity of the cloud data, and all service-based operational access are been provided to the corresponding data owner towards their specific cloud data. So the above said data owner access control strategies in-turn address issues that got raised due to intruder access to disturb financial statistics leads to denial of sustainability to regulate the illegal cloud resource consumption.

Keywords: - *CP-ABE, Access control, Public cloud storage, Accounting, Privacy-preserving.*

---***---

I INTRODUCTION

These days cloud computing became a vital solution for data-related service-based systems[1], especially cloud computing used for data as a service that addresses many data it needs in wide respect [3]. Where is in public clouds, data owner uploads data on to the cloud server which is kept under service by the cloud service provider to acquire security data owner after deciding to upload the data[6], first need to encrypt with the high standard encryption mechanism so that privacy preservation of data is been initiated at data owner end, this encrypted data then be sent to the cloud server wherein Cloud Service Provider has to control over this data and provides for facilitates for data user service access[5]. Data owner performs encryption with the secret key so that the same key is been used at the time of decryption at data users end, upon access permission control given by Cloud Service Provider, cipher-text oriented attribute-based encryption mechanism[4] increases the data privacy standards to acquire healthy relationship between data owner and Cloud Service Provider not letting the intruder to have access over it[8]. The data stored in the cloud server by data owner the private, economic info, identically strategies that need to be protected in higher levels enforcing persistent data storage establishing trusted Service data access model as well contributing white data accessibility limits with the proper authenticity evaluation mechanism please to get adapted to the current system needs[7]. So this private sensitive data of cloud data owner needs get safeguarded by Cloud Service Provider irrespective of policies privileged to the specific cloud data owner strategically[3]. The existing system that got empowered with access control strategies given by cloud server dominates the privacy protection policies in greater respects. So the proprietor of the data that is the data owner should have control over the data files that got stored by them specifically and there should be a situation to set access policy strategies by themselves to enhance the privacy standards thus reduces cloud Service Provider domination and intruder attacks over sensitive info of cloud data owner[10]. These confidentiality based access policies shouldn't be set by cloud Service Provider in a

DOI : 10.51319/2456-0774.2021.3.0016

generic way to all the cloud data owners in-turn a privilege given to a data owner in a specific way and the data owner could be in a situation to set the confidentiality access policy to every individual data resource separately which drastically increases privacy standards towards access policy mechanism as well increases the flexibility of access control at data owners end[9].

The objective of the Project:

The objective of this project is to facilitate data owner with high standards of privacy-preserving of sensitive data as well data confidentiality access policies has to be set by data owner itself in a resources Specific way. Along with that commercial aspect of denial of sustainability attacks by the intruder should be handled effectively and efficiently to increase trustability over the data source of the data owner.

Problem statement:

Especially in public clouds data resource of the data owner needs to get protected as it is a piece of private sensitive information, as well cloud Service Provider alone cannot grant access privileges to a specific data source of a specific data owner.

Scope of the Project:

In cloud computing data owner is a proprietor for their specific sensitive data to upload onto the cloud server and kept ready for data access services. So the data owner needs to convert original data into a cipher-text form to bring privacy protection as well data owner needs to assign an appropriate confidentiality data access policy to every individual data resource driven by them onto the cloud server.

Methodology:

Primarily in concern to the sensitive information of the data owner that got stored in the cloud server needs to get encrypted with a sophisticated approach like cipher-text oriented attribute-based encryption. Secondly, we need to address confidentiality access policies strategies that should get privileged to the data owner to their corresponding data resources by giving them a chance to choose personally by them.

II SYSTEM ANALYSIS

Existing System:

Especially in public clouds data resource of the data owner needs to get protected as it is private sensitive information, as well cloud Service Provider alone cannot grant access privileges to a specific data source of a specific data owner. In the existing cloud computing data handling approaches cloud server at most focuses on key management protocol policies and encourages data access in concern to that, more or less cloud Service Provider alone will organize the data access policies which in turn lacks control to data owners. Data resource of a cloud data owner is to be secured and safeguarded effectively by using appropriate encryption strategy which in turn may not have control over the resource access policies.

Drawbacks:

1.Lack of privacy preservation of data on a specific private sensitive data.

2.Data owner control over access policies is not been addressed

Proposed System:

The objective of this project is to facilitate data owner with a high standard of privacy-preserving of sensitive data as well data confidentiality access policies has to be set by data owner itself in a resources Specific way. Along with that commercial aspect of denial of sustainability attacks by the intruder should be handled effectively and efficiently to increase trustability over the data source of the data owner. Primarily in concern to the sensitive information of the data owner that got stored in the cloud server needs to get encrypted with a sophisticated approach like cipher-text oriented attribute-based encryption. Secondly, we need to address confidentiality access policies strategies that should get privileged to the data owner to their corresponding data resources by giving them a chance to choose personally by them.

Benefits:

1.privacy preservation of data on a specific private sensitive data is been handled at the Data owner's end effectively.

2.The data owner is privileged with specific access policies set by them to their specific Data resource.

III IMPLEMENTATION

There are four modules in this project. They are:

1.Data Owner

2.Data User

3.Cloud Server

Data owners:

The data owner is a proprietor of the data resource that has to be published on to the cloud server so that the resources data will be kept under service by the cloud server through cloud Service Provider. Who in-turn gets commercially benefited through resource utilization by data users, which should be managed by cloud Service Provider effectively.

Data users:

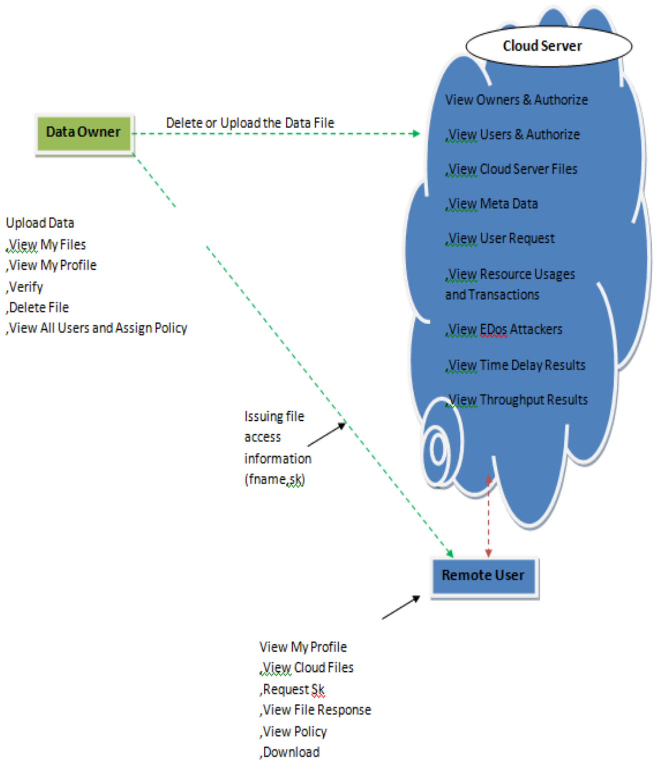
Cloud users are privileged to utilize the data resource supplied by the cloud owner under the supervision of the Cloud Service Provider. Every resource call needs to get evaluated by Cloud Service Provider to avoid Denial of service attacks. Authenticated cloud uses are effectively driven for cloud resource utilization fairly.

Cloud server:

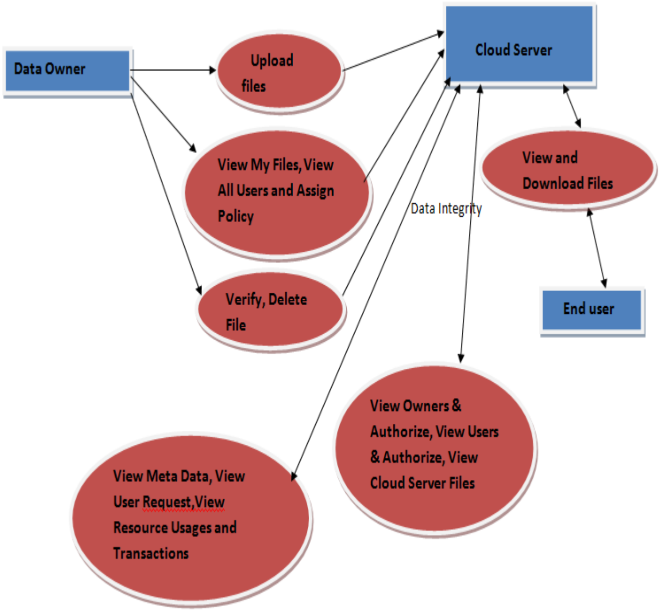
Cloud server hosts cipher-text encrypted data owners' sensitive data resources most effectively and also administrates data user access calls effectively and fulfils the commercial commitments over the specific data of cloud data owner.

IV SYSTEM DESIGN

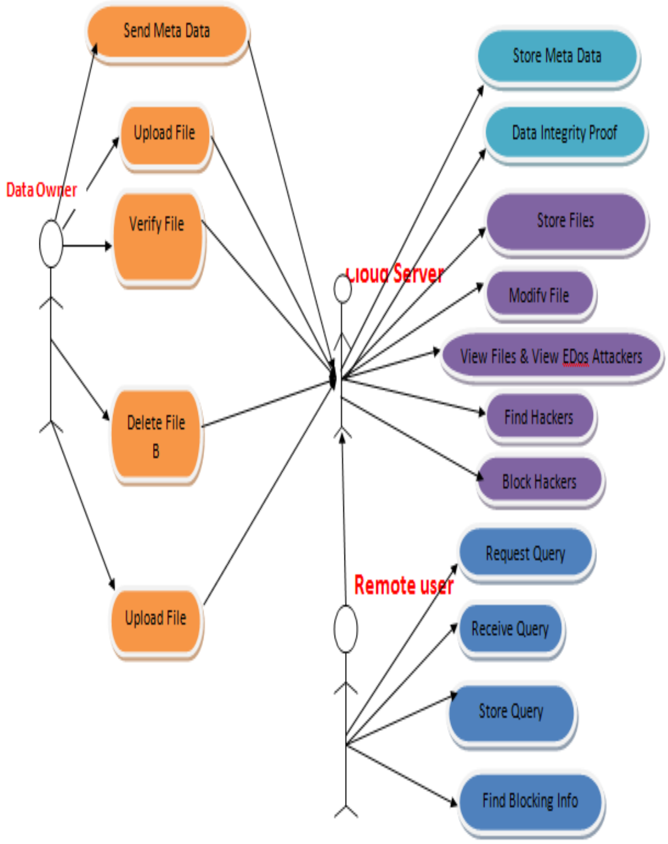
System Architecture:



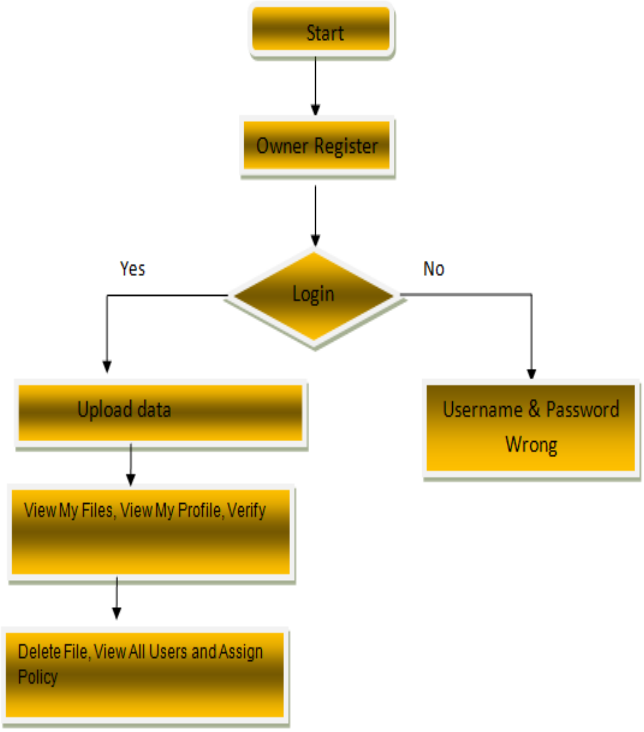
Data Flow Diagram:


Data Owner
Upload files
Cloud Server
View My Files, View All Users and Assign Policy
View and Download Files
Data Integrity
Verify, Delete File
End user
View Owners & Authorize, View Users & Authorize, View Cloud Server Files
View Meta Data, View User Request, View Resource Usages and Transactions

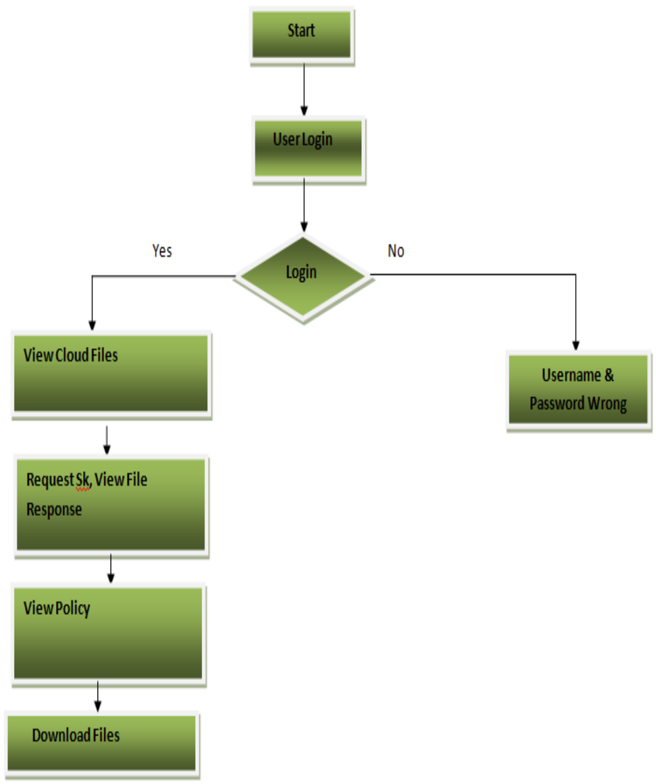
Use Case Diagram:



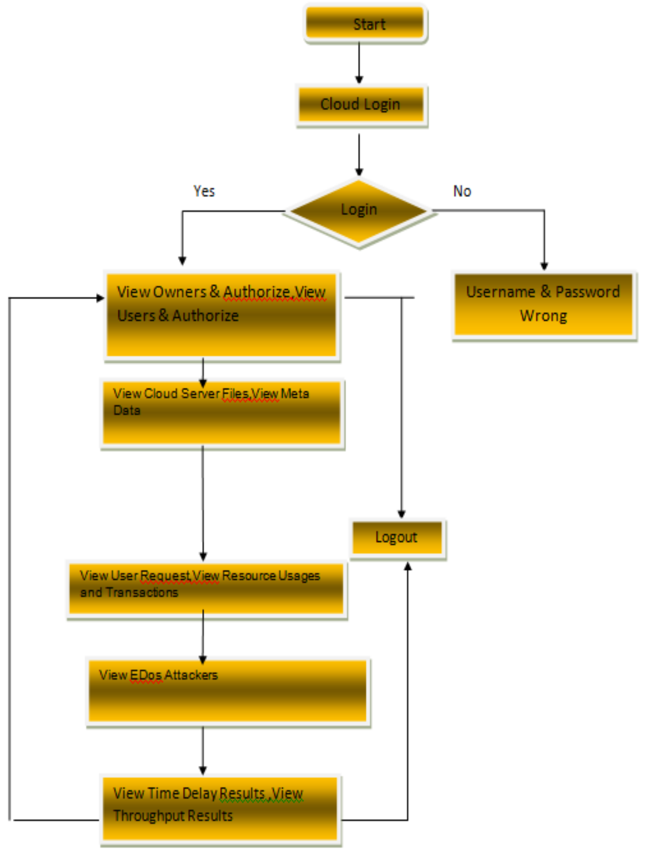
Flow Chart: Data Owner


Start
Owner Register
Login
Yes
No
Upload data
Username & Password Wrong
View My Files, View My Profile, Verify
Delete File, View All Users and Assign Policy

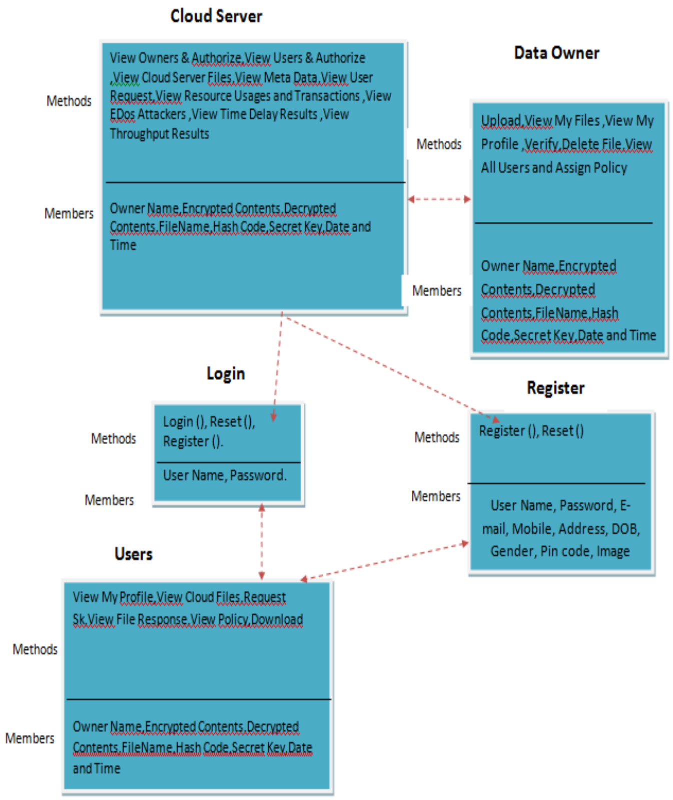
Flow Chart: User



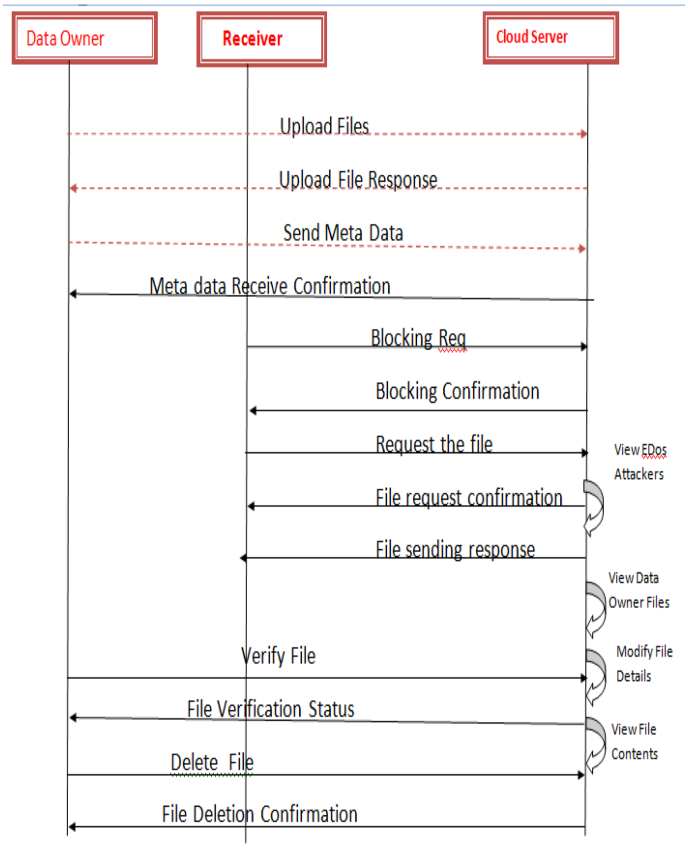
Flow Chart: Cloud Server


Start
Cloud Login
Login
Yes
No
View Owners & Authorize,View Users & Authorize
Username & Password Wrong
View Cloud Server Files,View Meta Data
Logout
View User Request,View Resource Usages and Transactions
View EDos Attackers
View Time Delay Results ,View Throughput Results

Class Diagram :


Cloud Server
Methods
View Owners & Authorize,View Users & Authorize ,View Cloud Server Files,View Meta Data,View User Request,View Resource Usages and Transactions ,View EDos Attackers ,View Time Delay Results ,View Throughput Results
Members
Owner Name,Encrypted Contents,Decrypted Contents,FileName,Hash Code,Secret Key,Date and Time
Data Owner
Methods
Upload,View My Files ,View My Profile ,Verify,Delete File,View All Users and Assign Policy
Members
Owner Name,Encrypted Contents,Decrypted Contents,FileName,Hash Code,Secret Key,Date and Time
Login
Methods
Login (), Reset (), Register ().
Members
User Name, Password.
Register
Methods
Register (), Reset ()
Members
User Name, Password, E-mail, Mobile, Address, DOB, Gender, Pin code, Image
Users
Methods
View My Profile,View Cloud Files,Request Sk,View File Response,View Policy,Download
Members
Owner Name,Encrypted Contents,Decrypted Contents,FileName,Hash Code,Secret Key,Date and Time

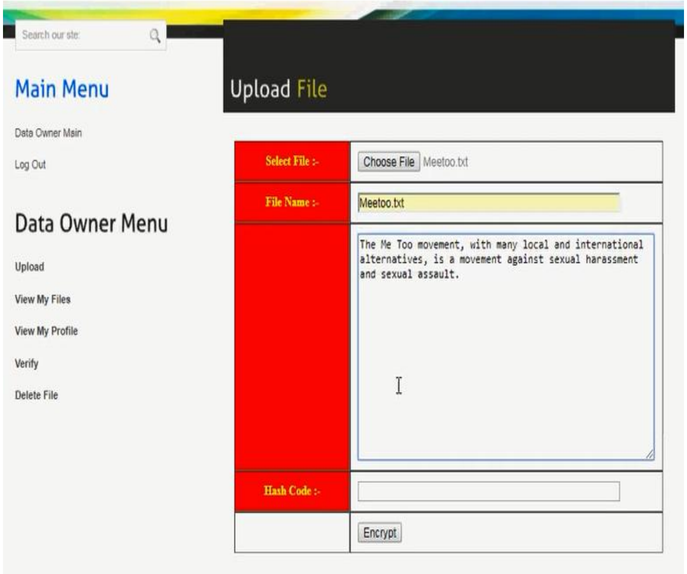
Sequence Diagram :



V PROJECT EXECUTION AND TESTING

Data Owner File Upload Page:

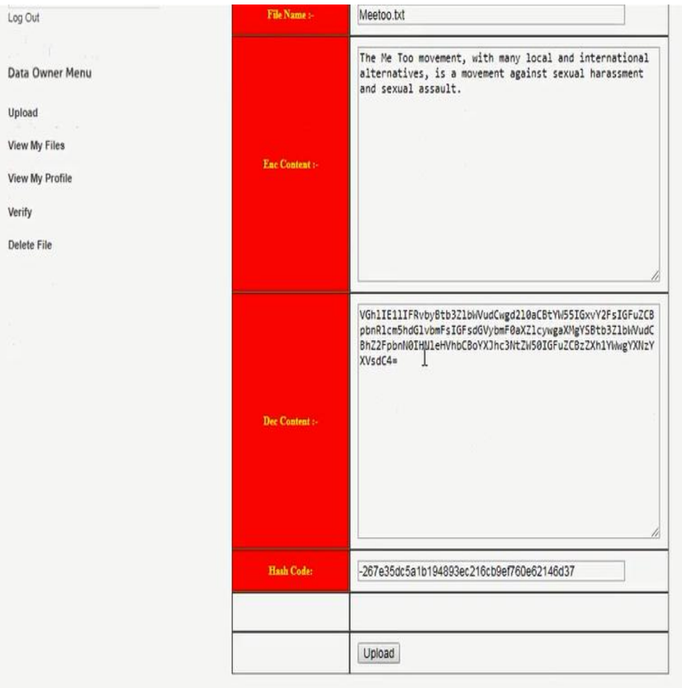
In this Data Owner File Upload Page data Owner can upload a file under service and then be encrypted so that privacy-preserving will be maintained at the data owner's end itself.



Select File :-	Meetoo.txt
File Name :-	Meetoo.txt
	The Me Too movement, with many local and international alternatives, is a movement against sexual harassment and sexual assault.
Hash Code :-	

Data Owner File Encryption Page:

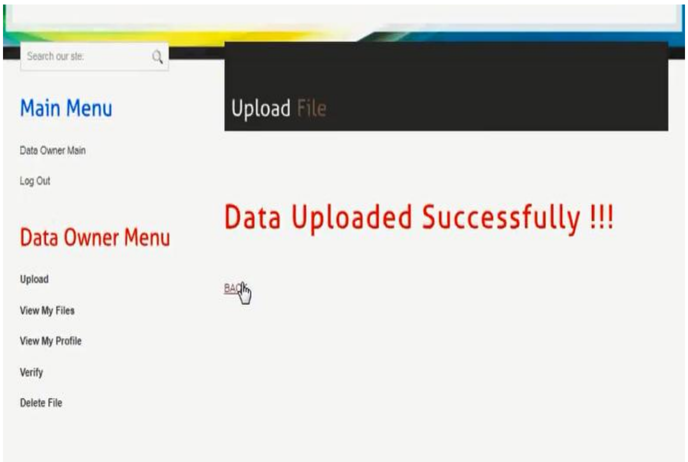
In this Data Owner File Encryption Page data, the Owner can upload a file under service needs to get through Encryption process on it. So that privacy-preserving will be maintained at data owners end itself.



File Name :-	Meetoo.txt
Enc Content :-	The Me Too movement, with many local and international alternatives, is a movement against sexual harassment and sexual assault.
Dec Content :-	VGhlIE1lIFRvbyBtb3ZlbWVudCwgd2l0aCBtYW55IGxvY2FsIGFuZCBpbnRlcm5hdGlvbmFsIGFsdGVybmF0aXZlcywgaXMgYSBtb3ZlbWVudCBhZ2FpbnN0IHNleHVhbCBoYXJhc3NtZW50IGFuZCBzZXh1YWwgYXNzYXVsdC4=
Hash Code:	-267e35dc5a1b194893ec216cb9ef760e62146d37

File upload Acknowledgement Page:

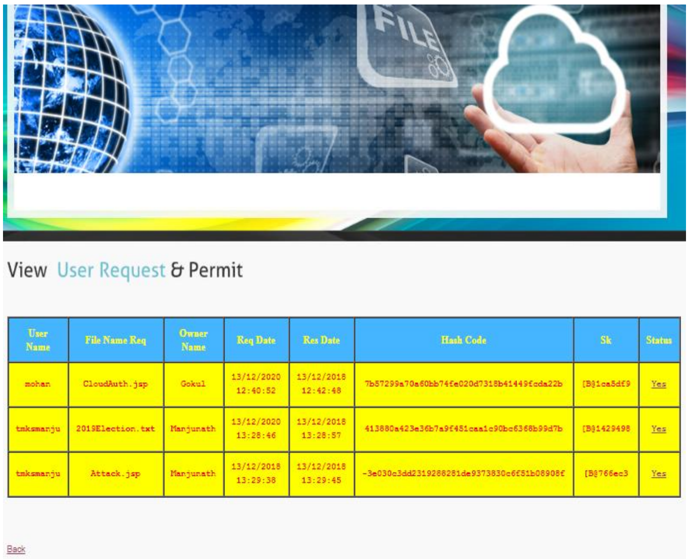
This is the file upload acknowledgment page that arises after successful uploading and encryption process initiated on the specific file by the data owner.



Data Uploaded Successfully !!!

User Request & Permission Page:

In this User Request & Permission page, the cloud Service administrator can view user requests and their corresponding status acknowledgment with a hyperlink.

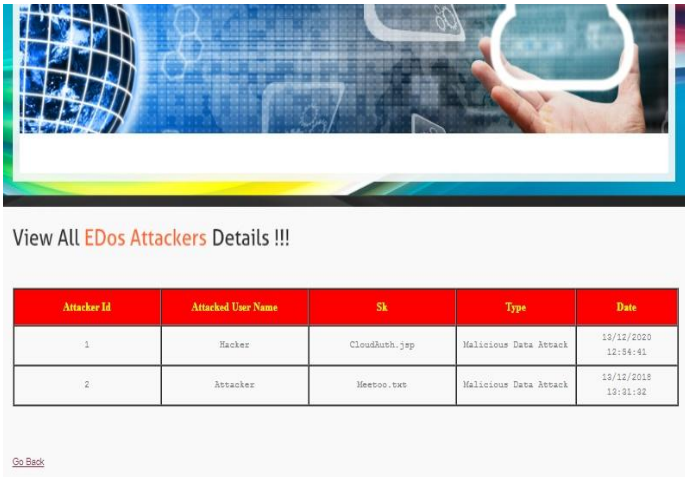


View User Request & Permit

User Name	File Name Req	Owner Name	Req Date	Res Date	Hash Code	Sk	Status
mohan	CloudAuth.jsp	Gokul	13/12/2020 12:40:52	13/12/2018 12:42:48	7b57299a70a60bb74fe020d7318b41449fcda22b	[B@1ca5df9	Yes
tmksmanju	2019Election.txt	Manjunath	13/12/2020 13:28:46	13/12/2018 13:28:57	413880a423e36b7a9f451caa1c90bc6368b99d7b	[B@1429498	Yes
tmksmanju	Attack.jsp	Manjunath	13/12/2018 13:29:38	13/12/2018 13:29:45	-3e030c3dd2319288281de9373830c6f51b08908f	[B@766ec3	Yes

EDos Attacks Page:

In this EDos Attacks Page, cloud Service administrators can view EDos Attackers' information in corresponding to a specific file.

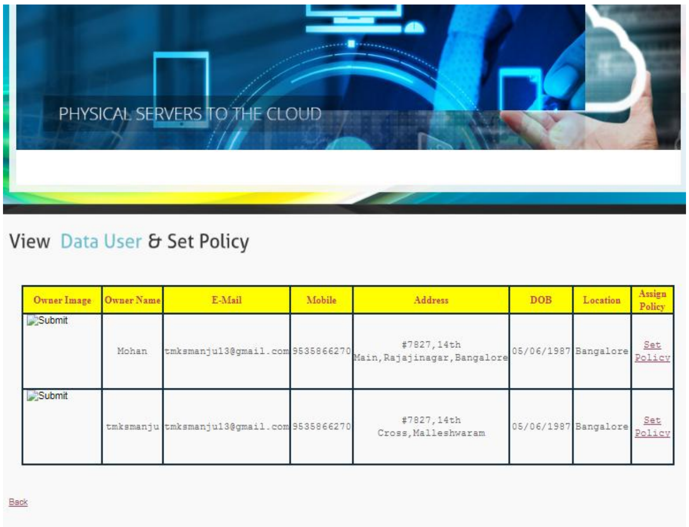


View All EDos Attackers Details !!!

Attacker Id	Attacked User Name	Sk	Type	Date
1	Hacker	CloudAuth.jsp	Malicious Data Attack	13/12/2020 12:54:41
2	Attacker	Meetoo.txt	Malicious Data Attack	13/12/2018 13:31:32

Access Policy Page:

In this Access Policy Page, the cloud Data Owner can view all user requests and can proceed to assign user-requested specific file access policy through a hyperlink.



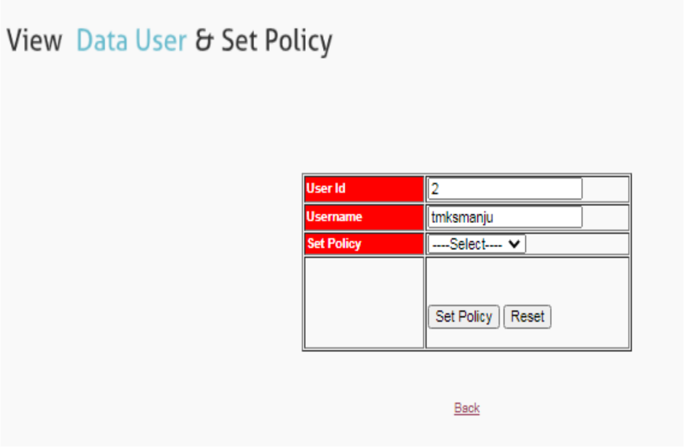
View Data User & Set Policy

Owner Image	Owner Name	E-Mail	Mobile	Address	DOB	Location	Assign Policy
Submit	Mohan	tmksmanju13@gmail.com	9535866270	#7827,14th Main,Rajajinagar,Bangalore	05/06/1987	Bangalore	Set Policy
Submit	tmksmanju	tmksmanju13@gmail.com	9535866270	#7827,14th Cross,Malleshwaram	05/06/1987	Bangalore	Set Policy

Back

Access Policy Assignment Page:

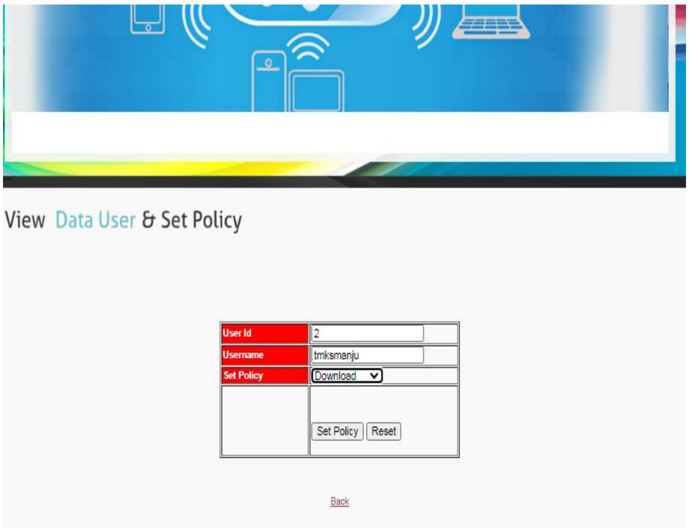
In this Access Policy, Assignment Page cloud Data Owner can set assigning one of the access policies like search, download & all attributes options to a user-requested specific file.



View Data User & Set Policy

User Id	2
Username	tmksmanju
Set Policy	----Select----

Back



View Data User & Set Policy

User Id	2
Username	tmksmanju
Set Policy	Download

Back

VI CONCLUSION

In this project, we recommended a cloud data controllability under supervised access policy mechanism through which security standards are been enhanced which leads to the establishment of trustable cloud-based data services effectively and efficiently. Initially, the data owner when he is uploading the file to put it on to ready for service situation will encrypt with an advanced mechanism and establishes a firm foundational security construct in a high manner. Putting aside the control of Cloud Service Provider over the data user request aside we adopt a new mechanism of cloud data control ability at cloud data owners end with a variety of options so that the reliability or trustability of the data on a specific data is been maintained effectively and efficiently. Thus in this project, we are successful in adopting both the methodologies that are related to privacy protection on data owner-specific files and supervision of data owner over their cloud data controllable access policies to safeguard private sensitive information of the cloud data owner. We also emphasize on EDos attack initiated by malicious intruders and established regulated system protocol to overcome the data leakages that may lead to the abnormality related to the commercial terms between the personalities of the cloud system.

Future Enhancement:

Apart from setting data confidentiality using a supervised access control mechanism that got facilitated to data owner module we could attempt for an enhancement by emphasizing on the system with a keen observation over the data that got uploaded by the data owner that has to get privacy protected and confidentiality maintained sensitive information. The whole data that has to get uploaded could be segmented into subsections so that data access policies could be separately assigned based on the privacy and security requirements of that block. By adopting this cloud Service Provider may need to maintain all these segmented access policies that got assigned in a proper dimensional structure which may be a typical process and need to get organized in a well-established manner.

REFERENCES

[1] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[2] Q. Zhang, L. Cheng, and R. Boutaba, “Cloud computing: state-of-the-art and research challenges,” Journal of Internet Services and Applications, vol. 1, no. 1,

[3] L. Zhou, Y. Zhu, and A. Castiglione, “Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner,” Computers & Security, vol. 69, pp. 84–96, 2017.

[4] V. Sekar and P. Maniatis, “Verifiable resource accounting for cloud computing services,” in Proceedings of the 3rd ACM workshop on Cloud computing security workshop. ACM, 2011, pp. 21–26.

[5] C. Chen, P. Maniatis, A. Perrig, A. Vasudevan, and V. Sekar, “Towards verifiable resource accounting for outsourced computation,” in ACM SIGPLAN Notices, vol. 48, no. 7. ACM, 2013, pp. 167–178.

pp. 7–18, 2010.

[6] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, no. 1, pp. 69–73, 2012.

[7] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in 2007 IEEE Symposium on Security and Privacy (SP’07). IEEE, 2007, pp. 321–334.

[8] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography– PKC 2011. Springer, 2011, pp. 53–70.

[9] S. Yu, K. Ren, and W. Lou, “Attribute-based content distribution with hidden policy,” in Proceedings of 4th Workshop on Secure Network Protocols (NPSec2008). IEEE, 2008, pp. 39–44.

[10] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, “Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data,” IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.