ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

Secured CP-ABE based An Efficient Concurrent Cloud Attestation

[1]ANURAGH VIJJAPU, [2] Dr. AMARAVATHI PENTAGANTI
[1]Ph. D Scholar, Department of CSE, NIILM University, Kaithal, Haryana.
[2]Professor, Department of CSE, NIILM University, Kaithal, Haryana.

ABSTRACT: In this paper the concept of attribute based encryption (ABE) is proposed for storing the data inside the drive HQ. Attribute based encryption had proposed to secure data storage. It provides the data security protection mechanism using this technique. Only a limited amount of data can be stored. The security of this concept is data integrity and confidentiality. Private keys and public keys are generated for accessing data from different sources. The user identify privacy in existing access control schemes so that private key generators are only responsible for generating keys and support the security concerned. Public key generators are not only responsible for storage point but also to identify the anonymous access from the user account. It supports to the user for providing access controls at the user end. Storage can be managed from administrator side easily which finds similar files inside the network storage system. By this it can be proved that it avoids duplicate storage and storage management also. It can also prove that ABE generates better results while comparing with cipher text policy attribute based encryption (CP-ABE).

Key Words: attribute based encryption, Cloud Attestation, Cipher, Text Policy, Cloud Server, Proxy,

Introduction: Encryption is very important these days because it helps every individual to protect their personal data from things like identity theft or information theft while the information is being transferred electronically. In similar way Government uses this encryption technique to secure the classified information. To prevent unauthorized user from accessing the information or data in the code is called encryption. So, by encoding a code or information only authorised person can get access to read it. There are three main reasons for encrypting the information. The first reason is, the actual information can be accessed by an authorised person only. Secondly, for the recipient the data remains unchanged. The recipient receives the data unchanged from the sender. Thirdly, The recipient can also be sure that the messages is coming from an authentic sender. The first reason of encrypting the message i.e. keeping the information secret is started in the military organizations and secret services during the world wars. But Julius caesar is the first person to use encryption. The encryption method is called caesar cipher which is named after him. He is used this method for his private correspondence. Secondly, it is established due to extensive use of internet for transmission of information in electronic form which is not a secure and trusted platform. So the purpose of encryption and decryption of information came into light. For example, when purchasing a product in an e-commerce website it redirects to the payment page. This page needs to more secure and trustworthy as bank details and card details are given here. So, this information should reach only to the person at the receiving end. It should be hidden from scammers to misuse that information. So, any details going though the internet must be secured by using the encryption process. Public keys and private keys They are the backbone of any exchange of information in electronic media through the internet. The recipient must maintain secrecy about the keys and should not share with any other people. In some cases they share these private and public keys with other people which is not trustworthy and safe. This leads to misuse of information or leaving the information for the un authorised users. These keys are generally long random numbers. These private and

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

public keys comprise of uniquely related cryptographic keys. By using the public accessing repositories the public keys are made available publicly as suggested in the name whereas, the private key is kept secret and accessible only by the person belongs to. An absolutely fundamental feature of private and public keys is that there is no direct relationship between them so that the private key cannot be calculated from the public key and vice versa. They do however have a special relationship where something in quoted by using the private key can only be decoded by using the public key and vice versa. So, whenever the information is encrypted by using the public key it can be decrypted by using the private key. If the information is encrypted by using the private key it can be decrypted by only using the public key.

Literature survey: At first it is suggested another Cipher text policy ABE strategy, using Cipher text policy ABE plots (Alam et al. 2016). In light of that scheme, we suggest a Cipher text policy ABE Plot that is re-appropriate and clearly safe for CPA. Starting at a late date, the first policy-based encryption chipboard program practiced in complete safety, (Li et al. 2017) Because we use the central framework of the Chipher Text Policy-Attribute Based Encryption.

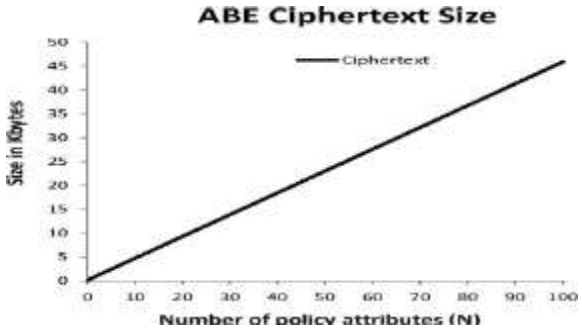

Figure 1 (a) Calculating cipher text

The ambiguity of the text structure influences both the decryption time and the cipher text size in a Cipher Text Politics-ABE scheme. We create cipher text strategies in the form of (A1, A2……AN) circumstance over the approach), where Ai is an Attribute.

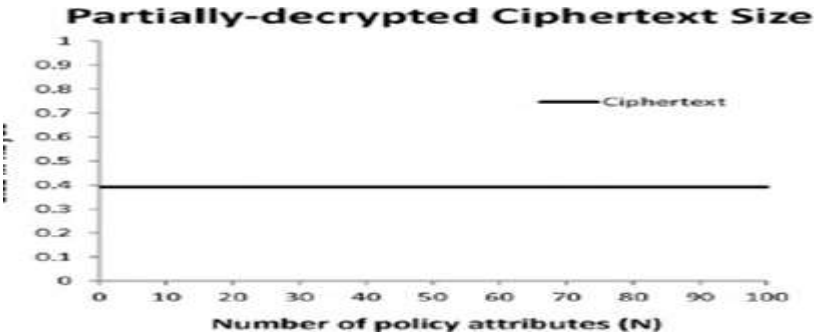

Figure 1(b) Partially Decrypted Ciph 1

The above Diagram represents the entire System will be depends upon the security if the secure decryption fails immediately the encrypted text doesn't support to decrypt properly.

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

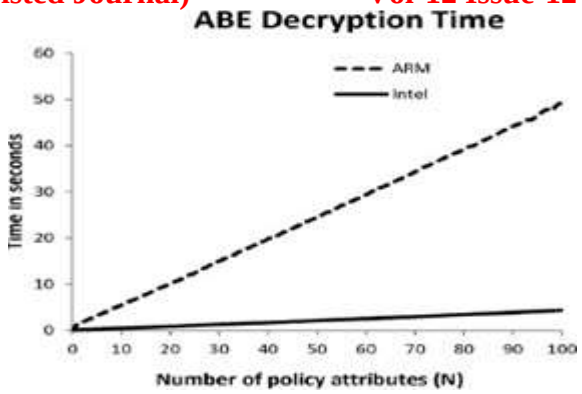

Figure 1 (C) Cipher Text Policy-At 1

It shows the result of completely decrypted text time and the attributes only allows to user after generated keys.

Cipher text policy ABE System with Outsourced Decryption Include a cloud-based electronic remedial record system that guarantees valuable patients information use decentralized cloud-based encryption schemes based on the Cipher Text Policy attribute. To help you find a workable speed records on your (Ferreira et al. 2015) With the ultimate objective of saving enlisting cost, the mediator could reestablish a medicinal record changed heretofore for a comparable authority Because of system breakdown or malignant ambush, the go- between could send the helpful record of another patient or an archive of the correct structure in any case, passing on erroneously information.

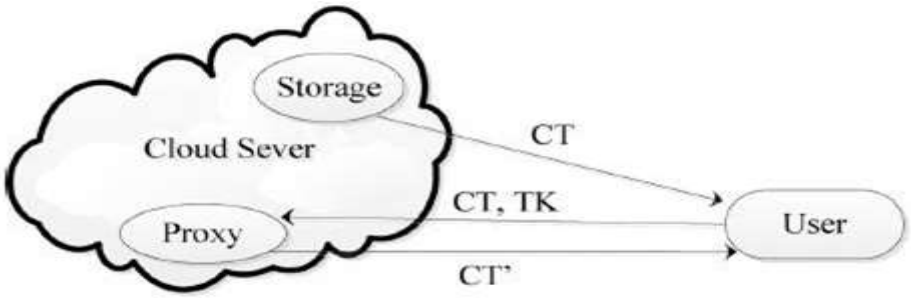

Figure 2 Cipher Text Policy-Attribut 1

Cipher Text policy-attribute-oriented encryption with redistributed scrapping: in Cipher Text policy-attribute-based encryption a client outfits a cloud with a modifier that allows cloud uncross (Singh et al. 2017) Figure message on message into an important comparable figure message, without anything about it. It triggers the likelihood of re-encryption by the middle party. Delegated recryption allows the mid-way individual using an encoding key to change the (Xue et al. 2016) message. We underscore that in the model of go-between encryption; confirmation of the go between's change can't be developed. This can be quickly clarified as looks for after. An arbiter could supplant the encryption of under Alice's open key with the encryption of another message under Alice's open key and after that utilization its re encryption key to change the last into an encryption of under Bob's open key. Doubtlessly, without investment with Alice, Bob can't see this compromising conduct of the center individual.

Hybrid Cipher text policy ABE Scheme with CCA: This concept propose a solid circuit cipher text-arrangement characteristic based crossover encryption with certain assignment plan dependent on the multi linker maps and the undeniable processing innovation under cloud condition. We give a short portrayal of the

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

convention Authority creates private keys for the information proprietor also, client. The information proprietor scrambles his information utilizing mixture encryption framework, creates a secretly obvious Macintosh for each symmetric cipher text and afterward transfers the entire cipher text to the cloud server. By then the data owner could be detached. The customer, who needs to access to the data, speaks with the cloud server. The ran jolts exhibit that the value is moved clandestinely, while the solid jolts show that the value is moved without an ensured channel Utilizing general circuits to communicate the passageway control approach, we manufacture a monotone circuit with significance l and data size to be n.

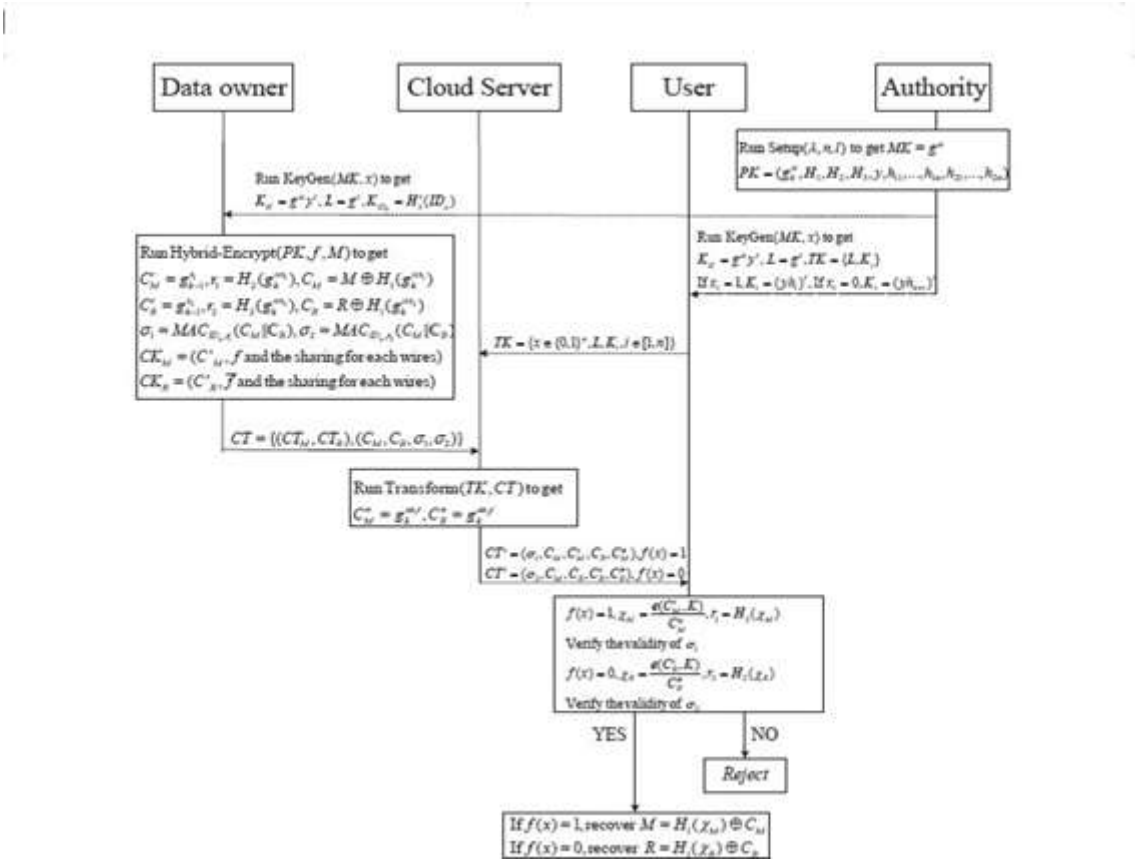

Figure 3 Hybrid Cipher text policy ABE scheme in cloud

In the above diagram Data owner is responsible to store the content with Trusted Authority; from cloud server data user can get the data if the data is relevant to his/her not need the data owner permission for access it.

Attribute based key-approach:-

Characterized key-approach attributes Based encryption Cipher Text Policy-(KP-ABE) as well as the Cipher Text Policy-Attribute Simple encryption as two complementary forms of ABE. The monotonic control systems were the key improvements made to KP-ABE, In any case, It recognize that KP-ABE (Ali et al. 2017). is less flexible than Cipher text policy ABE considering the way that the entry framework is settled once the client's property private key is given. Since message- shot encryption can't keep up a vital good ways from to savage force ambushes where records falling into an acknowledged set will be recouped, a structure that gives secure de replicated limit confining mammoth force assaults was advanced by perceived framework called server-helped encryption.

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

PROPOSED DESIGN: These chapter explain the design and storage of the data inside cloud server, the server needs to posses two thing the content should be in encrypted format or not and also it should have to check the data along with the keys are generated or not. It supports to delete the duplicated copies inside the server, its worked based upon the content based checking concept, it takes two parameters as verifying the data one is file name and the file size.

Phase 1 Design:

For phase 1 implementation of our cloud storage system, the following sections describe the use case diagrams, functional requirements and detailed activity diagrams. More specifically, the focus is on the activities to be stored by the cloud server.

Cloud Server Storage System Use case Diagram

Figure 4.1 Displays the Cloud service storage case diagram. This defines the case / activities used in such storage by the cloud server.

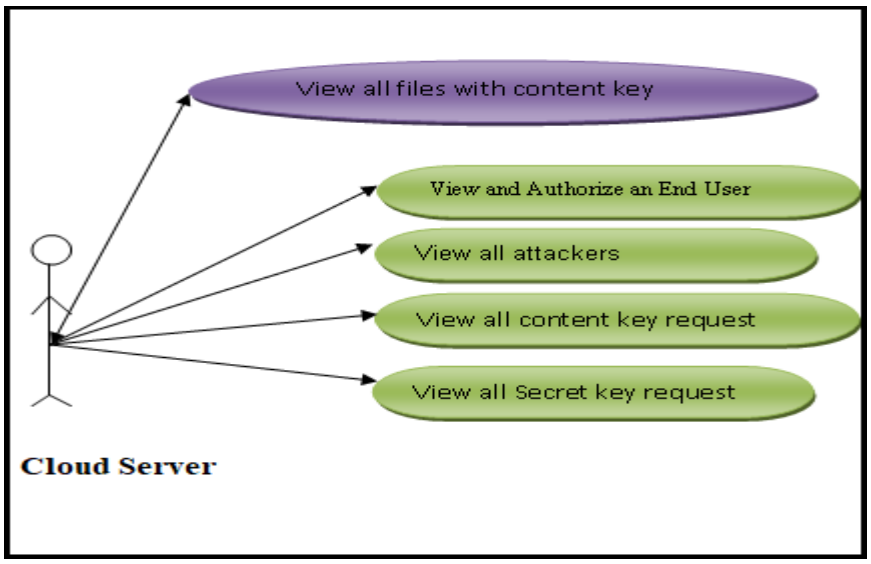

Figure 4.1: Phase 1 Use Case Diagram for cloud server storage system

Cloud server must view all the files with the content key, authorize end user, can view all the attacker files along with the content key request and secret key request.

Functional Requirements:

Technical specifications must be met before the cloud framework evaluation starts (Bourne et al.2017). Functions must be fulfilled by a cloud server, customer and data holders. Every cloud server has the following technical requirements:

Data Owner Functional Requirements:

Data Owner must have to register with in the server, then only server administrator generate accessibility to owner for storing the files inside the cloud servers. The Owner need the content Master secret key for browsing the plain text after that generated encrypted file allowed inside the cloud server. Data Owner uploading file to cloud with tag , label and security key.

Data User Functional Requirements:

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

Data User must have to register with in the server, then only server administrator generate accessibility to user for retrieving file from cloud server. The Data user need the content key and file response for downloading content.

Cloud server Functional Requirements:

It permits the checked information by the cloud server executive and permits documents inside the DriveHQ. We are utilizing MySQL as an essential stockpiling framework and Drive HQ as an optional stockpiling framework right now. Secure De duplication with the objective of sparing extra room for distributed storage administrations, Douceur et al the primary answer for adjusting privacy and proficiency in performing de duplication called merged encryption, where a message is scrambled under a message-determined key so indistinguishable plaintexts are encoded to a similar figure writings. Right now, two clients transfer a similar document; the cloud server can observe the equivalent figure messages and store just one duplicate of them.

Sequence Diagram:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

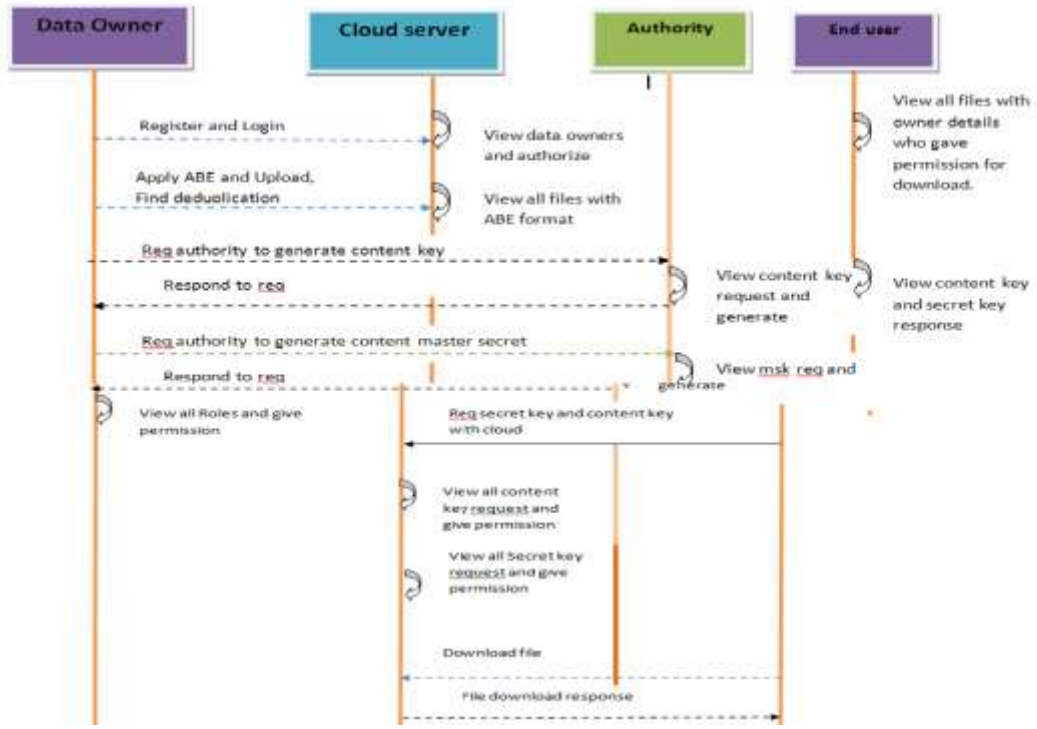

Fig4.2: sequence diagram

Results: This project implemented the concept of Data storage system and remove duplicate copy entry from cloud server. The key generation system supports the controlling of each file and uploading and downloading strategy so the security protection mechanism applied on the data storage system. It created some users are super users like authority, cloud those are only applicable to take functionalities from the data user, data owner. Authority is a fixed user means we are not registering, through data base username and password we are login. In same case cloud server also login with data base username and password. Authority login success he/she can perform generating master key, generating content key, view files with owner details and

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

keys. For the user to provide data cloud server is responsible, searching facility; response only authorized files, View owner details, and user details. Cloud server can generate the content key, master key for the user. Cloud server can view the total transaction and can delete from cloud server all files at a time.

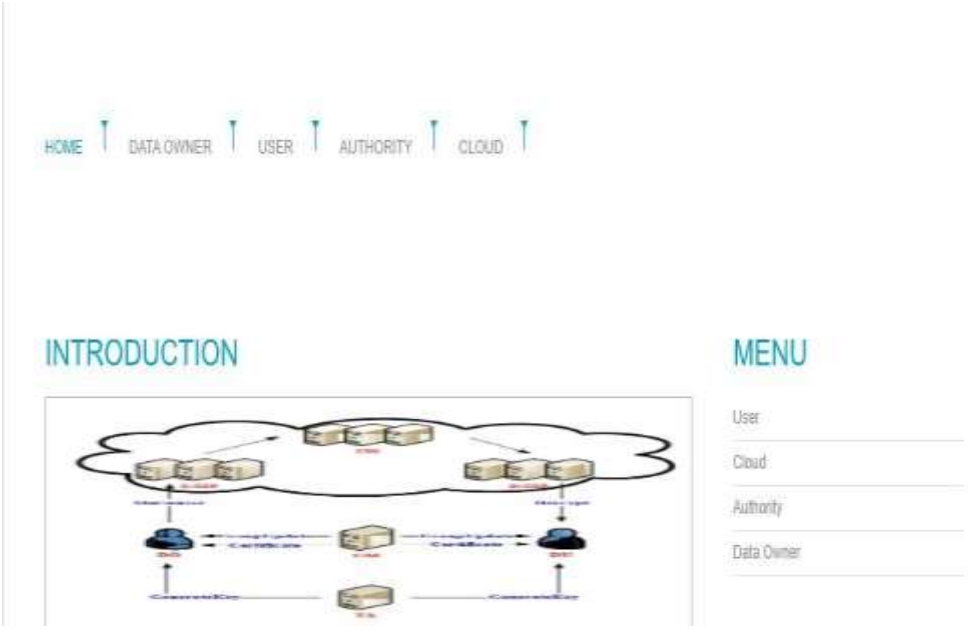

Fig: user, owner, authority and cloud server

The above diagram is Home page it shows all the navigation for user, owner, authority and cloud server.

Data Owner Performance: In this section data owner creation performance we are recording while data creation depending upon the fields those is mandatory fields for retrieving and accessing information related from tables. So the concept of security applying through data owner section Cloud server can check is the data owner registered or not if not ask the feedback form to data owner to register. If login success stores the content inside cloud server and also find the de duplication of file in cloud.

Fig: Registration page for the data owner

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

The above screen for the registration page for the data owner, he/she filling the form then after clicking on register

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

The request fill receive at the business logic then after content or the fields relevant data stored into the database.

In above Image we are retrieving the data by using the above fields those are id,name,pass,email,mobile,addr,dob,gender,pin,location,status,image and those will supports to receive the information from data owner,

Data Owner Login

Data Owner login with the username and passwords those are very confidential for the data owner and using this owner can performed some activities like storing and checking file whether those are secure from cloud are not.

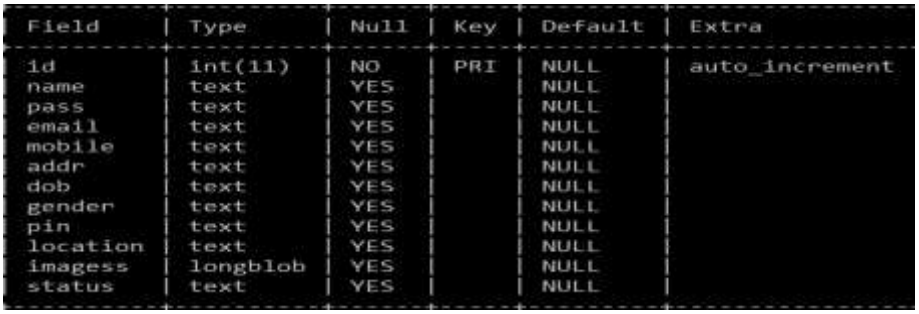

Fig: The describe table of data owner

When data owner login to the web site the values are taken from the downer table.

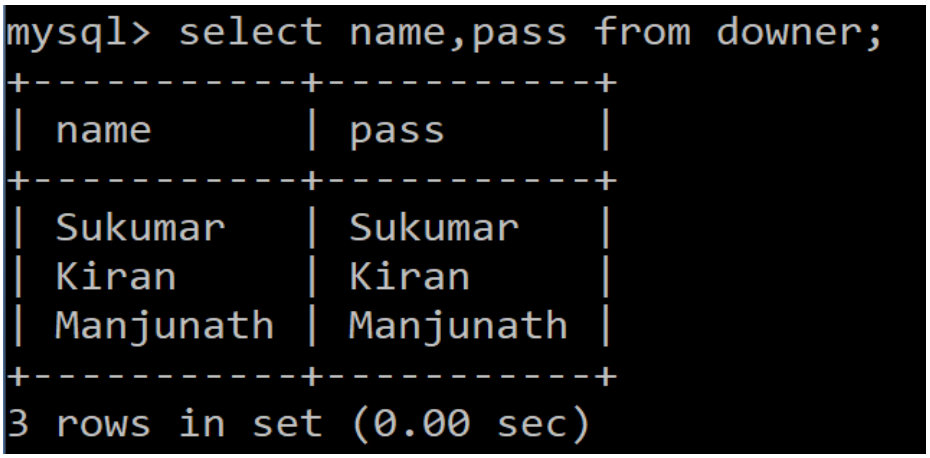

Fig: The select Query for user name, password of downer

After registration done by the downer database administrator can check the data on cmd line argument of MySQL server.

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

The data viewing right only having to Database administrator so data owner should have to know the username and his/her password before login.

After one successful login data owner gets the relevant user wall page using these page the data linking performance apply.

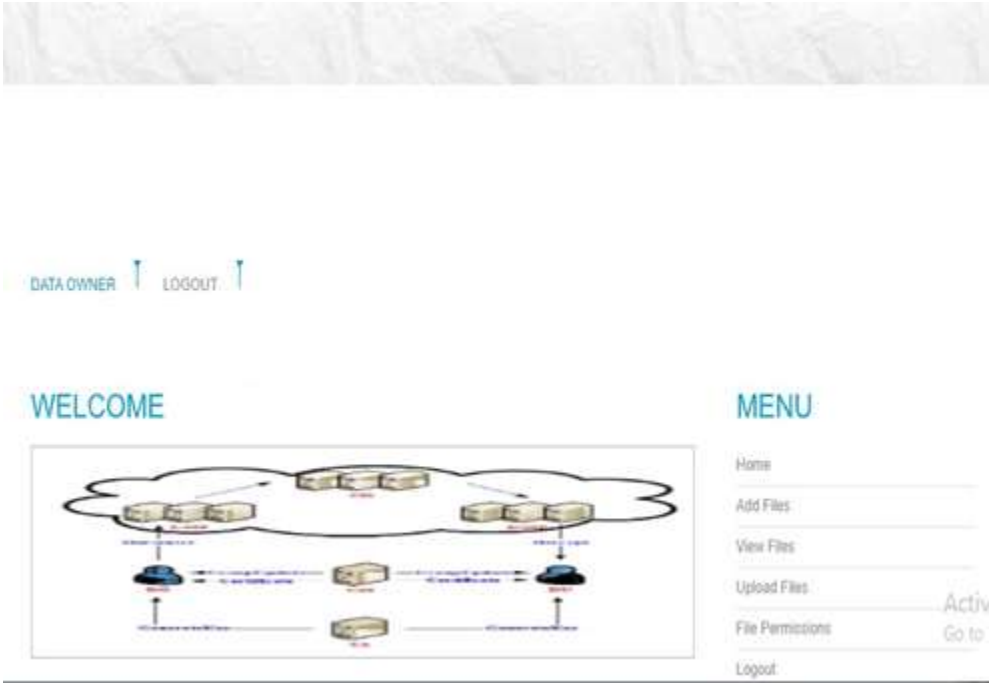

Fig: Welcome Page after successful login

After login success data owner can add file to content server then after upload the file into cloud server also give the file access permissions to the relevant users.

Add Files Section

Using this section data owner can choose his/her files for adding the data to the container after the cloud operation then only its applied inside the driveHQ storage.

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

Fig: Upload contents

After the clicked on the add file button file added to container then the success page displayed.

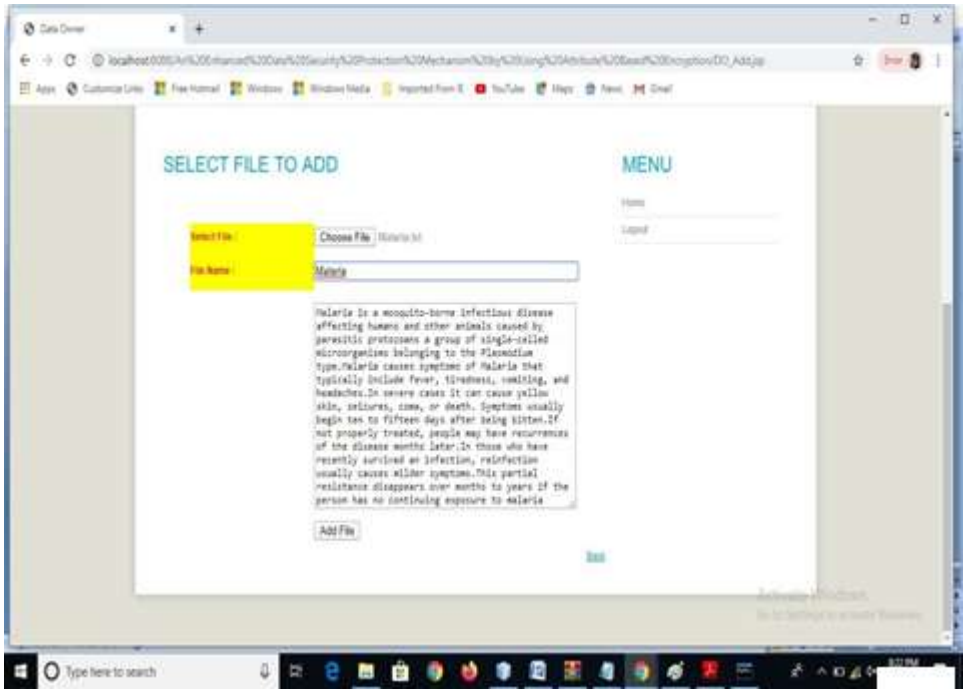

Fig: Browser view of data uploading

In the above page we have the browse section after clicked on it data added to the text area section then it looks like above screen.

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

```
mysql> desc ownerfiles;
+------------+---------+------+-----+---------+----------------+
| Field      | Type    | Null | Key | Default | Extra          |
+------------+---------+------+-----+---------+----------------+
| id         | int(11) | NO   | PRI | NULL    | auto_increment |
| fname      | text    | YES  |     | NULL    |                |
| ct         | text    | YES  |     | NULL    |                |
| secretkey  | text    | YES  |     | NULL    |                |
| contentkey | text    | YES  |     | NULL    |                |
| rank       | int(11) | YES  |     | NULL    |                |
| dt         | text    | YES  |     | NULL    |                |
| downer     | text    | YES  |     | NULL    |                |
+------------+---------+------+-----+---------+----------------+
```

Fig(c) The Describe table of owner files

In this table user having the file with 8 parameters for adding files those are supported for displaying the relevant information about secret key and content key.

```
mysql> select id,fname,secretkey,contentkey,rank from ownerfiles;
+----+------------+------------+------------------+------+
| id | fname      | secretkey  | contentkey       | rank |
+----+------------+------------+------------------+------+
|  4 | Dengue.txt | [B@d7b7d9  | sl19x0vf0k3q3p2k |    0 |
|  7 | Cancer.txt | [B@11415c8 | qi89t4ul3u0o4o8i |    0 |
|  8 | Dengue     | No         | No               |    0 |
|  9 | Maleria    | No         | No               |    0 |
+----+------------+------------+------------------+------+
4 rows in set (0.00 sec)
```

Fig (d) Data applied on owner files

Automatic rank generation process applied on different file content the status secret key, content key is No means its not generated by someone else that why the generation of the secret key and content key duty is given to other users.

Conclusion: For cloud computing concept the concept of ABE is applied. It is proved that the data is encrypted and is in a secure format. More than open process we are trying to make available to the proposed system. Data provider can just take relax about the data security why because no data loss from the cloud server .Data Outsourcing is in data owner hand and data sets control can be maintained easily also de duplication process applied on loaded Information the availability of data can view at the cloud server level. The attribute based encryption not only removing duplication files it's also providing benefits for the business providers to maintain valuable cloud storage. Cloud engineering's are worked on stockpiling framework to maintain secure de duplication data. Private clouds are calculating the storage capacity and displaying remaining storage availability inside the infrastructure. Trapdoors are generated by the private clouds those are dependent upon the generated cipher text, depends upon cipher text user can access data more than once in secure manner and can decrypt the

data. We can also view the relevant data in the form of plain text. Private cloud can maintain the data accessing information and provide the data to the relevant user and control invalid accessing. Private cloud maintains evidence from invalid accessed data user. The calculations done by the private cloud based on labels and generates similar results on the cipher text. After attacker tried to get the cipher text and it will not decrypted by the received credentials need the permission from cloud server that is in the form of trapdoor. Finally, It showed how attribute based storage be practically integrated within existing dispersed storage systems. Proposed scheme provides a possible way to fight against immoral interference with the right of privacy.

References:

1. Ali, M., Dhamotharan, R., Khan, E., Khan, S.U., Vasilakos, A.V., Li, K., Zomaya, A.Y. (2014) SeDaSC: Secure Data Sharing in Clouds, IEEE Syst. J.(2015).
2. Ali, M., Dhamotharan, R., Khan, E., Khan, S.U., Vasilakos, A.V., Li, K., Zomaya, A.Y. (2017) 'SeDaSC: Secure Data Sharing in Clouds', IEEE Systems Journal, 11(2), 395–404.
3. Androulaki, E., Soriente, C., Malisa, L., Capkun, S. (2014) 'Enforcing Location and Time-Based Access Control on Cloud-Stored Data', in 2014 IEEE 34th International Conference on Distributed Computing Systems, Presented at the 2014 IEEE 34th International Conference on Distributed Computing Systems, 637–648.
4. Arora, R., Parashar, A. (2013) 'Secure User Data in Cloud Computing Using Encryption Algorithms'.
5. Arora, R., Parashar, A., Transforming, C.C.I. (2013) 'Secure user data in cloud computing using encryption algorithms', International journal of engineering research and applications, 3(4), 1922– 1926.
6. Bethencourt, J., Sahai, A., Waters, B. (2007) 'Ciphertext-policy attribute- based encryption', in 2007 IEEE Symposium on Security and Privacy (SP'07), IEEE, 321–334.
7. Cai, K., Hong, C., Zhang, M., Feng, D., Lv, Z. (2013) 'A secure conjunctive keywords search over encrypted cloud data against inclusion-relation attack', in 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, IEEE, 339–346.
8. Chen, J., Ma, H. (2014) 'Efficient decentralized attribute-based access control for cloud storage with user revocation', in 2014 IEEE International Conference on Communications (ICC), IEEE, 3782– 3787.
9. Cui, H., Deng, R.H., Li, Y., Wu, G. (2019) 'Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud', IEEE Transactions on Big Data, 5(3), 330–342.
10. Fan, K., Tian, Q., Wang, J., Li, H., Yang, Y. (2017) 'Privacy protection based access control scheme in cloud-based services', China Communications, 14(1), 61–71.
11. Ferreira, B., Rodrigues, J., Leitão, J., Domingos, H. (2019) 'Practical Privacy-Preserving Content-Based Retrieval in Cloud Image Repositories', IEEE Transactions on Cloud Computing, 7(3), 784– 798.

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

12. Fu, Z., Ren, K., Shu, J., Sun, X., Huang, F. (2015) 'Enabling personalized search over encrypted outsourced data with efficiency improvement', IEEE transactions on parallel and distributed systems, 27(9), 2546–2559.
13. Fu, Z., Sun, X., Ji, S., Xie, G. (2016) 'Towards efficient content-aware search over encrypted outsourced data in cloud', in IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications, IEEE, 1–9.
14. Hong, J., Xue, K., Li, W., Xue, Y. (2015) 'TAFC: Time and Attribute Factors Combined Access Control on Time-Sensitive Data in Public Cloud', in 2015 IEEE Global Communications Conference (GLOBECOM), Presented at the 2015 IEEE Global Communications Conference (GLOBECOM), 1–6.
15. Hur, J. (2011) 'Improving security and efficiency in attribute-based data sharing', IEEE Transactions on Knowledge and Data Engineering, 25(10), 2271–2282.
16. Karame, G.O., Soriente, C., Lichota, K., Capkun, S. (2019) 'Securing Cloud Data Under Key Exposure', IEEE Transactions on Cloud Computing, 7(3), 838–849.
17. Lang, B., Wang, J., Li, M., Liu, Y. (2018) 'Semantic-based Compound Keyword Search over Encrypted Cloud Data', IEEE Transactions on Services Computing, 1–1.
18. Li, J., Ma, R., Guan, H. (2017) 'TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud', IEEE Transactions on Cloud Computing, 5(1), 126–139.
19. LI, R., Shen, C., He, H., Gu, X., Xu, Z., Xu, C.-Z. (2018) 'A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing', IEEE Transactions on Cloud Computing, 6(2), 344–357.
20. Liu, J.K., Liang, K., Susilo, W., Liu, J., Xiang, Y. (2015) 'Two-factor data security protection mechanism for cloud storage system', IEEE Transactions on Computers, 65(6), 1992–2004.
21. Liu, J.K., Liang, K., Susilo, W., Liu, J., Xiang, Y. (2016) 'Two-Factor Data Security Protection Mechanism for Cloud Storage System', IEEE Transactions on Computers, 65(6), 1992–2004.
22. Liu, Q., Tan, C.C., Wu, J., Wang, G. (2011) 'Reliable re-encryption in unreliable clouds', in 2011 IEEE Global Telecommunications Conference-GLOBECOM 2011, IEEE, 1–5.
23. Poon, H.T., Miri, A. (2015a) 'An efficient conjunctive keyword and phase search scheme for encrypted cloud storage systems', in 2015 IEEE 8th International Conference on Cloud Computing, IEEE, 508–515.
24. Poon, H.T., Miri, A. (2015b) 'A low storage phase search scheme based on bloom filters for encrypted cloud services', in 2015 IEEE 2n International Conference on Cyber Security and Cloud Computing, IEEE, 253–259.