EFFICIENT SECURE DATA RETRIEVAL ON CLOUD USING MULTI-STAGE AUTHENTICATION AND OPTIMIZED BLOWFISH ALGORITHM

Dileep P [1], Tirupati Rao S [2], Revathy P [3]
[1] Professor, Department of Computer Science and Engineering
[2] Associate Professor, Department of Computer Science and Engineering
[3] Assistant Professor, Department of Computer Science and Engineering
[1] Malla Reddy College of Engineering and Technology,Kompally,Hyderabad,India.
[2] Geethanjali College of Engineering and Technology,Keesara,Hyderabad,India.
[3] Narsimha Reddy Engineering College,Kompally,Hyderabad,India.

ABSTRACT

Cloud computing is currently playing an important role in the information technology industry because of its improved efficiency, wide access, low cost, and many benefits. It also provides more space for storing data and transmitting data from one location to another faster for different users on the Internet. Due to large storage, cloud customers can save huge capital investment on IT infrastructure and focus on their own core business. Therefore, many companies or organizations are moving their business to the cloud. However, many customers are reluctant to use the cloud due to security and privacy concerns. To tackle this problem, in this paper, efficient secure data retrieval is developed with the help of multi-stage authentication (MSA) and optimized bluefish algorithm (OBA). The proposed system consists of three modules namely, MSA, data security, and data retrieval. Initially, the cloud users register their information on cloud based on a multi-authentication procedure. After the registration process, the data are encrypted with the help of OBA. To increase the security of the system, the key value is optimally selected with the help of a binary crow search algorithm. After the encryption process, MSA based data retrieval process is performed. This will avoid, unauthorized person to attack the data. The performance of the proposed methodology is implemented in JAVA and performances are analyzed in terms of different metrics.

INTRODUCTION

In recent years, cloud computing (CC) has made great strides in the technology industry and the scientific community (De la Prieta et al. 2019). CC is a computing model that can be used anywhere, anytime. They only pay the amount based on usage. This method is called pay-as-you-go fashion (Kumar et al. 2019). Storage is one of the most influential and needed computing resources in the current digital era. It is one of the most popular services in the CC industry (Helmi et al. 2018). Due to a large amount of storage, a lot of organizations and industries store their data on the cloud. Amazon's Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3) and apple cloud are well-known examples of cloud data storage. However, security is a major issue in cloud computing. To overcome the security problem, a lot of cryptography algorithms and access control mechanisms are introduced. Security goals are set at three points namely, confidentiality, integrity, and availability. Cryptography is concerned with the confidentiality of data in the cloud

To access the cloud storage data, the access control mechanism is utilized. Access control technology can not only ensure the valid access requests of valid users but also prevent the invasion of unauthorized users, as well as address security issues caused by the misuse of valid users. Traditional access control is identity-based authentication technology and operates within the confines of a unified security domain (Vafamehr and Khodayar 2018; Li et al. 2009). For access control mechanisms, single authentication, biometric authentication, and multi authentications methods are developed. The single-stage authentication approach may steal. Bio-metric authentication namely, fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina authentication have been proposed in the literature. Each biometric accreditation program has its advantages and disadvantages, which are based on several factors, such as sustainability, individuality, and acceptability (Kushida and Pingali 2014; Burger 2001). One of the main drawbacks of using bio-metrics is its intrusion into the user's character. Besides, most biometric systems require a special scanning device to authenticate users, which does not apply to remote and Internet users. To avoid the problem, multi-stage authentication (MSA) is developed. The MSA consists of more than three security layers (Kang et al. 2015, Dinesha and Agrawal 2012; Rajani et al. 2016).

Similarly, recently, many cryptography-based secure data transaction is presented namely, Advanced Encryption Standard (AES) (Sachdev and Bhansali 2013), Data Encryption Standard (DES) (Ramya et al. 2016), Rivest, Shamir, & Adleman (RSA) (Somani et al. 2010), SHA-256 (Sundarakumar and Mahadevan 2019), elliptical curve cryptography (ECC) (Bai et al. 2017) and blowfsh algorithm (Reddy et al. 2015) etc. multi stage authentication based security also introduced. Even though, some problems namely, maximum execution time, cost, and information loss are not reduced. The meta heuristics algorithm also developed to improve the performance of cryptography algorithms. To avoid the problem, an efficient new algorithm is needed to solve the security issues

The main objective of the proposed methodology is to securely transmit the data on the cloud using MSA and optimized bluefish algorithm (OBA). MSA is three-stage security layers that avoid unauthorized users access the data on the cloud. The proposed works have developed based on dual security layers such as MSA based access control and cryptography algorithm. In the authentication process, MSA is developed. In MSA, if any Stage Client does not provide the information correctly, he will be rejected immediately. Thus, no unknown person can take the information from the storage center. After the authentication process, data are encrypted using OBA. Here, the key values are optimally selected using binary crow search algorithm (BCSA). Finally, the user retrieves the data, if they satisfy the multiple authentication processes. In this manner, unauthorized users are avoided. The main contribution of the paper is listed below;

To encrypt the data blowfsh algorithm is utilized. To enhance the blowfsh algorithm, key values are optimally selected using BCSA. This will hide the original information from malicious.

- To avoid the malicious login process, MSA process is proposed. This will secure the provider from malicious.

LITERATURE SURVEY

A lot of research has been developed to secure data transactions on the cloud. Among them some of the works are analyzed here; Cheng et al. (2018) had developed an Identity-Based Encryption (IBE) based accountable privacy-preserving mechanism on CC. Initially, based on the privacy attributes accountable privacy-preserving mechanism is presented. Second, the proposed accountability for CC involves the privacy-protecting mechanism, the proposed accounting, and auditing approaches. The experimental of the proposed methodology is analyzed in terms of diferent metrics. In Sudhakar and Rao (2020), Sudhakar et al. had developed a secure aware data transaction on the cloud using an index based quasi–identifer approach. Here, they utilized an incremental and distributed data set for experimentation. Here, initially, input data are clustered with the help of modified fuzzy c-means clustering (MFCM). Then tuple partitioning is done. After that, important data are selected from the clustered output. To avoid sensitive data loss, data are secured with the help of Bucketization.

with the help of Bucketization. Brindha and Shaji (2018) had developed a conditional source trust attributes encryption mechanism with particle swarm optimization (CSTAE-PSO) based secure data transaction on the cloud. Here, initially, condition attributes are selected and then, the selected attributes are encrypted with the help of the CSTAE mechanism. In this paper, to increase the performance of the encryption process, the bilinear mapping transformation function was included in CSTAE. To attain the minimal transaction with completion time, the PSO algorithm was developed. The performance of the proposed methodology was analyzed in terms of different metrics namely, throughput level on the transaction, security rate on the data layer, and transaction completion time.

Kanna and Vasudevan (2019) had developed a hybrid crypto mechanism-based privacy preservation on the cloud. The crypto mechanism was designed based on a fully homomorphic–elliptic curve cryptography (FH-ECC) algorithm. Initially, DO encrypt the information using the ECC algorithm. To improve the security of the data, again data was encrypted with the help of a fully homomorphic (FH) algorithm. After encryption process data was stored on the cloud. After the storage process, the access control policy was developed to avoid the unauthorized person login. The performance of the proposed methodology was analyzed in terms of different measures namely, execution time, encryption time, and decryption time. Moreover, Mohiuddin et al. (2019) had developed adaptive bin packing algorithm based secure data storage on the cloud. Here, they introduced an end to end security framework for data at rest in cloud storage to eliminate insider threats. The security threads were identifed and performance was analyzed.

Pournaghi et al. (2020) had explained a block chain and attribute based encryption is developed. In this paper, they securely store the medical data on cloud. To avoid the unauthorized person login process, fne-grain access control mechanism is utilized. Moreover, Sumathi and Sangeetha (2020) had developed a data security on cloud. In this paper, the security issues are reduced by Group Key Based Attribute Encryption using Modifed Random Fibonacci Cryptographic (MRFC).initially, the input data was separated into sensitive and non-sensitive data using attribute segregation method. Then, the sensitive data are encrypted using MRFC. The performance of this approach is analyzed in different metrics. Pragaladan and Sathappan (2018) had developed Combining DNA Structure and Multi-aspect Time-Integrated Cut-of Potential based secure data storage on cloud. This method was reducing the time complexity for establishing confidentiality of the data. This framework improves the authentication level of security by using confidentiality and authentication techniques from unauthorized user change.

Resende et al. (2015) had explained a Physical Unclonable Function (PUF)-based mutual multi factor entity and transaction authentication for secure banking. Here, PUF with Password-based Authenticated Key Exchange (PAKE). Using this method, only parties authenticated in the current session can valid bank transactions. Tsai and Su (2020) had explained the authentication of online banking customers and transactions through use of a hash-based multi-server authentication scheme in conjunction with a smart card. The proposed system provides strong security features and low maintenance costs for financial institutions’ Internet banking platforms. The proposed mechanism was associated with a customized interface and thus easily integrated into existing banking systems for use in Internet banking applications. Moreover, Guo et al. (2019) had explained a block chain algorithm based security for online education classes.

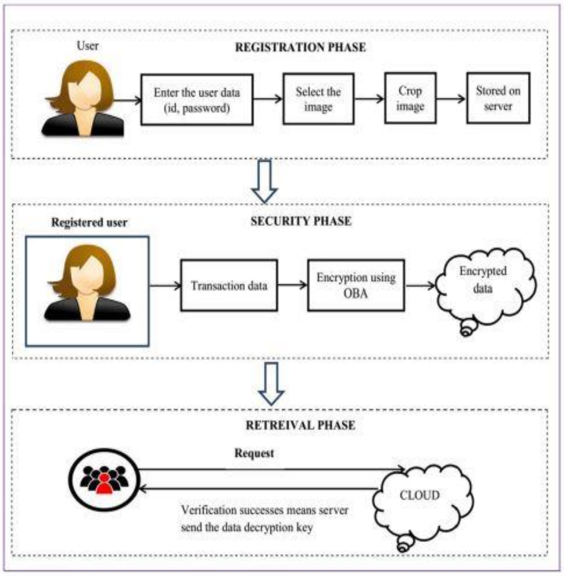
PROPOSED SECURE DATA TRANSACTION ON CLOUD

Cloud computing is a service that has been rapidly increasing its growth in the information technology industry in recent years. Privacy and security are challenging issues for cloud users and providers. In a public cloud environment, users cannot control its remote data as it transfers its data to a public cloud server. Therefore, information security is a critical issue in public cloud storage, such as confidentiality, integrity, availability, and reliability of data. To resolve this issue, in this research, an OBA as well as MSA is proposed. OBA aims to strengthen sensitive data confidentiality in public cloud storage. The proposed method consists of three stages namely, MSA, data security using OBA, and query-based data retrieval. In this method SaaS is used. This method prevents the data into insider attacker and outsider attackers. The overall diagram of the proposed methodology is given in Fig. 1

The proposed methodology consists of three phases namely, registration phase, security phase and retrieval phase. In the registration phase, users are registered their information on cloud. In this phase, to avoid the unauthorized person login process, MSA is developed. In the security phase, the data are encrypted using Blowfsh algorithm. To enhance the bluefish, the encryption keys are optimally selected using BCSO algorithm. In the retrieval phase, authorized persons are given the request to the server. The user is registered means, they will receive the data otherwise the request will neglect.

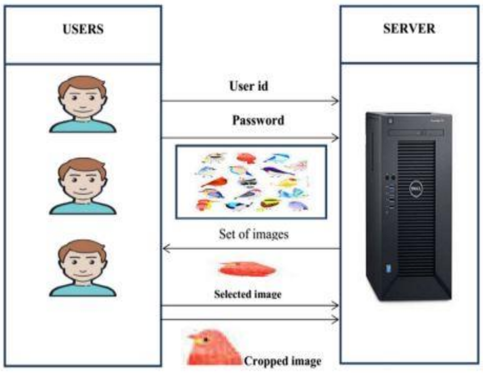
MSA process

The authentication process is crucial to avoid data loss, data theft, and malicious attack. Especially in a centralized environment, unauthorized clients can easily transfer data without the owner's knowledge, meaning that a security breach is inevitable. To avoid this problem, in this paper, MSA is proposed to securely access the data on the cloud. It will protect cloud assets against unauthorized access by enforcing access control mechanisms. The MSA process contains two stages such as registration and login. The detail explanation is given below;



Registration process

Registration process In the registration stage, clients have entered their information on data centre. At frst, the client generates the user id Uid, password Pid, and entering all the information about the user. After receiving the Uid and Pid, the server shows N several images to the client. Among the N number of images, the user selects one image I1. Then, the selected image is sent to the server and stored. Then, to further enhance the authentication, the selected image I1 is cropped and the cropped area is sent to the server. This also stored on the server.



Login process

In this section, the login process is explained. Once the registration is done successfully, the client can upload or download data to the cloud. Without the registration process, no one client retrieves any information to the cloud. Using this process, we can avoid data loss. For login, at first, clients enter their information such as user id Uid and password Pid . After receiving the information, the server checks if the given information is correct or not. If it is correct means, the server immediately displays N number of images. The registered image also included in the displayed images. From the images, the client selects one image. This image is the same as the registered image means, the process is continued. Otherwise user request it neglected. After the image selection process, the client crops the same image and sends it to the server. Then, the server checks the similarity between the cropped image and registered crop image. If it is matched means, the server allows the client to access the data, otherwise, they neglect the request

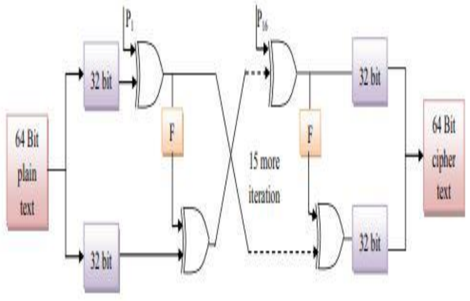
Data security using the optimized bluefish algorithm

After the registration process, the input data is encrypted by using an OBA. The Blowfsh Algorithm (BA) is the symmetric key cryptography algorithm. The key length of the 64-bit block is 32–448 pieces (Meyers and Desoky 2008). Here, P-array and four 32-bit S-boxes are available. The S-boxes recognize 8-bit information with convey 32-bit yield. BA has two main stages, namely the key expansion and encryption process. For the encryption process, a 16 round steel network is used. Each round has a main dependency permutation and a key-dependent substitution. All functionality is to add 32-bit words in XOR and BA

Consider the plaintext value is 123456abcd132536. The step by step procedure of bluefish algorithm is given as

Generate key size

- Initialize sub situation box
- Encryption
- Decryption



The need for data protection particularly in shared environment and in multi-tenant environments been a primary consideration among customers. In shared environment storage and network resources needs some technologies to protect data in cloud computing, Some surveys identified security is one of the main challenge in implementing cloud computing solutions. Users store sensitive information such as financial data, regulated industries such as health care and public utilities in cloud and cloud will operate external service providers and challenges in achieving security issues. Some solutions are applicable to verify security acquiescence in cloud environment they are inconsistent, scalability, effectiveness. Many organizations deploy their software in fixed hardware infrastructures and noncore applications in the public cloud and some organizations are building their own private clouds. Some of the security challenges include those of physical layer, virtualization layer and in cloud layer. Security experts mainly concentrate on data isolation issues and address them using pervasive encryption. However from the past few years the cloud computing has made a lot of changes in IT industry even large companies Google, Microsoft are also struggled a lot to provide powerful, cost efficient and reliable cloud platforms. It is more flexible to the users so that many users make use of the cloud leads to various network and information security risks in cloud computing. In cloud computing the client's data is distributed across different networks and stored the client's data in data centers and the data resides in the physical network of service providers. Service providers cover from unexpected security attacks and vulnerabilities when the data is uploaded and offloaded to and from the cloud data centers.

Efficient Secure Data Retrieval on Cloud using Multi-Stage Authentication and Optimized Blow fish Algorithm

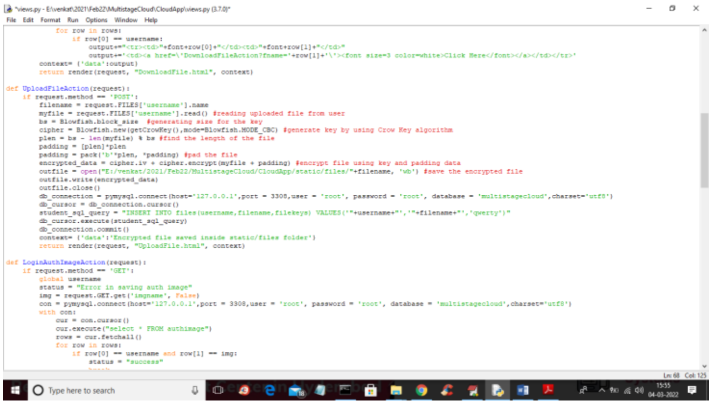
Now-a-days all organizations such as Online Social Networks, Healthcare Banking and many more are migrating their applications to cloud environment as cloud servers will provide heavy storage and computation in cheaper cost but still some organizations are hesitating to store their data in Cloud due to security issues as their data are saved at 3rd party cloud servers away from their reached and cloud servers or attackers may hack and misuse that data.

To overcome from this problem many encryption and authentication techniques such as biometric verification are introduced but this require extra devices or hardware and existing AES algorithms require heavy computation and to overcome from this problem author of this paper introduce novel concept called multi-stage authentication with efficient data storage and retrieval using optimized Blow fish security algorithm.

This paper consists of 3 modules such as authentication, data security and retrieval Blow fish algorithm is optimized for efficiency by applying Crow search algorithm for key generation and selection where selected keys fitness will be evaluated to check it should not easy to hack. Multi-stage authentication is applied by allowing user to get register with the application by giving username and password and then display list of images to user and then user has to select one image from the list and this image get cropped and store in database.While login multi authentication is applied by asking user to enter username and password and if login successful then display list of images and user has to select correct image given at registration and if correct image is selected then only allow user to upload and download file.

OPERATION:

Below code showing data encryption with key generation using Blowfish algorithm



views.py - E:\venkat\2021\Feb22\MultistageCloud\CloudApp\views.py (3.7.0)

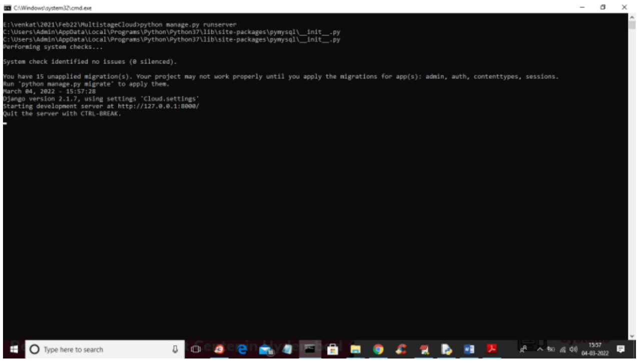
```
            for row in rows:
                if row[0] == username:
                    output+="<tr><td>"+font+row[0]+"</td><td>"+font+row[1]+"</td>"
                    output+='<td><a href=\'DownloadFileAction?fname='+row[1]+'\'><font size=3 color=white>Click Here</font></a></td></tr>'
        context= {'data':output}
        return render(request, "DownloadFile.html", context)

def UploadFileAction(request):
    if request.method == 'POST':
        filename = request.FILES['username'].name
        myfile = request.FILES['username'].read() #reading uploaded file from user
        bs = Blowfish.block_size  #generating size for the key
        cipher = Blowfish.new(getCrowKey(),mode=Blowfish.MODE_CBC) #generate key by using Crow Key algorithm
        plen = bs - len(myfile) % bs #find the length of the file
        padding = [plen]*plen
        padding = pack('b'*plen, *padding) #pad the file
        encrypted_data = cipher.iv + cipher.encrypt(myfile + padding) #encrypt file using key and padding data
        outfile = open("E:/venkat/2021/Feb22/MultistageCloud/CloudApp/static/files/"+filename, 'wb') #save the encrypted file
        outfile.write(encrypted_data)
        outfile.close()
        db_connection = pymysql.connect(host='127.0.0.1',port = 3308,user = 'root', password = 'root', database = 'multistagecloud',charset='utf8')
        db_cursor = db_connection.cursor()
        student_sql_query = "INSERT INTO files(username,filename,filekeys) VALUES('"+username+"','"+filename+"','qwerty')"
        db_cursor.execute(student_sql_query)
        db_connection.commit()
        context= {'data':'Encrypted file saved inside static/files folder'}
        return render(request, "UploadFile.html", context)

def LoginAuthImageAction(request):
    if request.method == 'GET':
        global username
        status = "Error in saving auth image"
        img = request.GET.get('imgname', False)
        con = pymysql.connect(host='127.0.0.1',port = 3308,user = 'root', password = 'root', database = 'multistagecloud',charset='utf8')
        with con:
            cur = con.cursor()
            cur.execute("select * FROM authimage")
            rows = cur.fetchall()
            for row in rows:
                if row[0] == username and row[1] == img:
                    status = "success"
```

In above screen read red colour comments to know about Blowfish algorithm

SCREEN SHOTS

To run project first create database in MYSQL by copying content from 'database.txt' file and paste in MYSQL

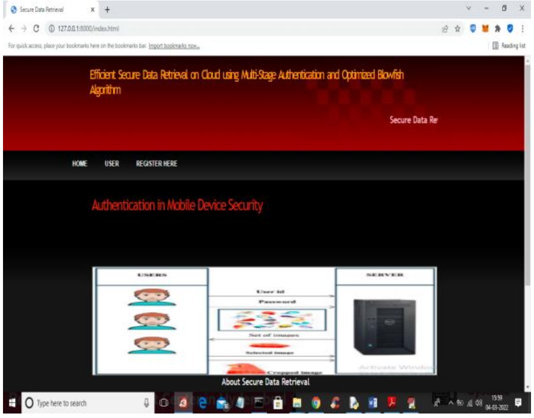
Now double click on 'runServer.bat' file to start server and get below screen



C:\Windows\system32\cmd.exe

```
E:\venkat\2021\Feb22\MultistageCloud>python manage.py runserver
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
Performing system checks...

System check identified no issues (0 silenced).

You have 15 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin, auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
March 04, 2022 - 15:57:28
Django version 2.1.7, using settings 'Cloud.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

In above screen server started and now open browser and enter URL as http://127.0.0.1:8000/index.html and press enter key to get below screen



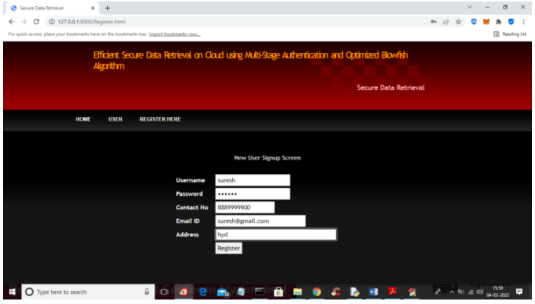
Efficient Secure Data Retrieval on Cloud using Multi-Stage Authentication and Optimized Blowfish Algorithm

Secure Data Re

Authentication in Mobile Device Security

About Secure Data Retrieval

In above screen click on ‘Register Here’ link to allow user to register



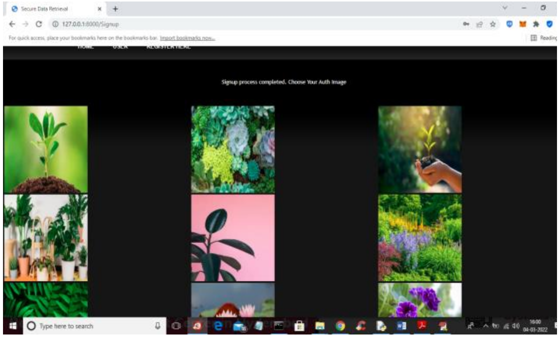
Efficient Secure Data Retrieval on Cloud using Multi-Stage Authentication and Optimized Blowfish Algorithm

Secure Data Retrieval

New User Signup Screen

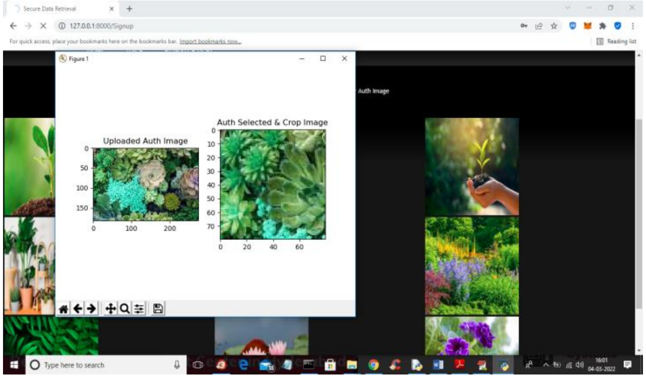
Username: suresh
Password: ••••••
Contact No: 8889999900
Email ID: suresh@gmail.com
Address: hyd

In above screen user is enter sign up details and then click on ‘Register’ button o get below images screen

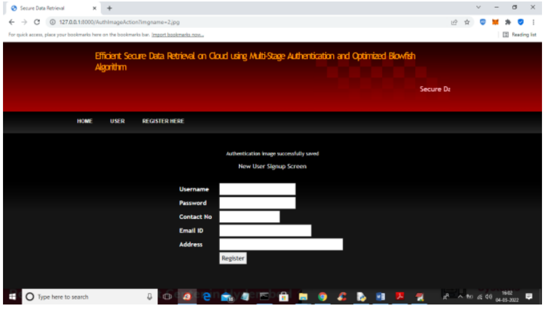


Signup process completed. Choose Your Auth Image

In above screen user has to click on desired image as second authentication and to get below output



In above screen user can see selected and cropped image and then close above image to store on server and to get below screen



Efficient Secure Data Retrieval on Cloud using Multi-Stage Authentication and Optimized Blowfish Algorithm

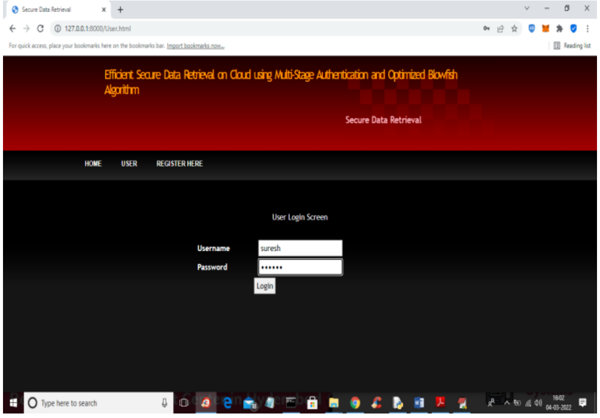
Secure Da

Authentication image successfully saved

New User Signup Screen

Username
Password
Contact No
Email ID
Address

In above screen sign-up process completed and now click on ‘User’ link to get below login screen



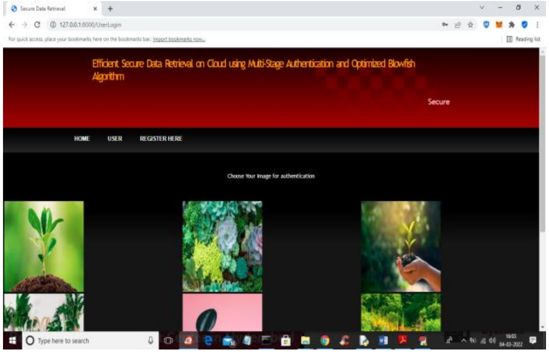
Efficient Secure Data Retrieval on Cloud using Multi-Stage Authentication and Optimized Blowfish Algorithm

Secure Data Retrieval

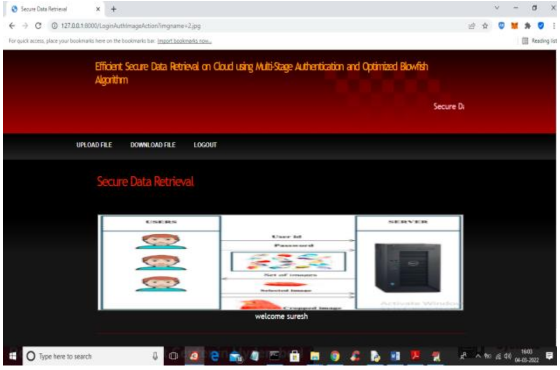
User Login Screen

Username: suresh
Password: ••••••

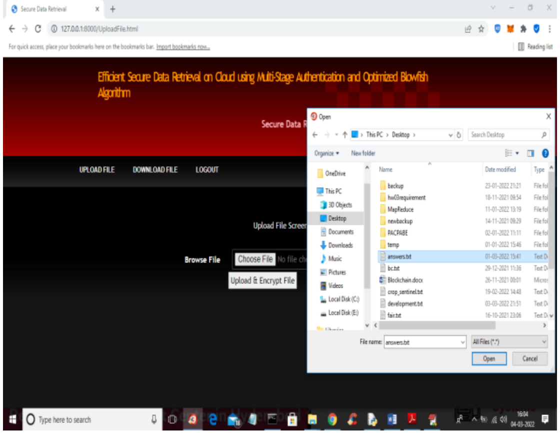
In above screen as first authentication user has to enter login details and press button to get below screen


Efficient Secure Data Retrieval on Cloud using Multi-Stage Authentication and Optimized Blowfish Algorithm
Secure
HOME
USER
REGISTER HERE
Choose Your Image for authentication

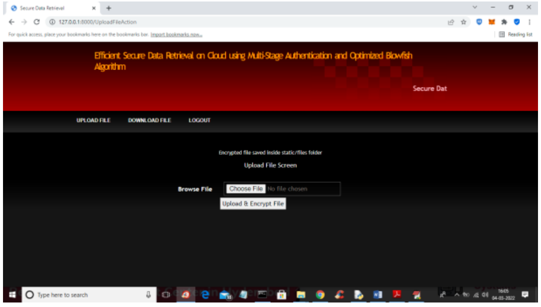
In above screen user has to click on correct image as second authentication and if image is authenticated then will get below output


Efficient Secure Data Retrieval on Cloud using Multi-Stage Authentication and Optimized Blowfish Algorithm
Secure Di
UPLOAD FILE
DOWNLOAD FILE
LOGOUT
Secure Data Retrieval
welcome suresh

In above screen user has click on 'Upload File' link to get below screen



In above screen selecting and uploading file and then click on 'Open and Upload & encrypt' button to get below screen

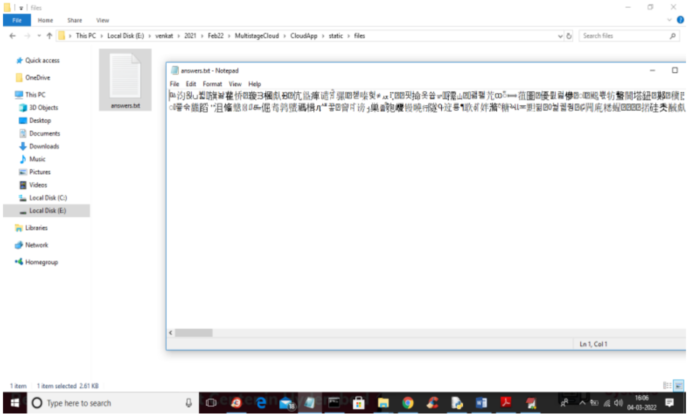

Efficient Secure Data Retrieval on Cloud using Multi-Stage Authentication and Optimized Blowfish Algorithm
Secure Dat
UPLOAD FILE
DOWNLOAD FILE
LOGOUT

Encrypted file saved inside static/files folder

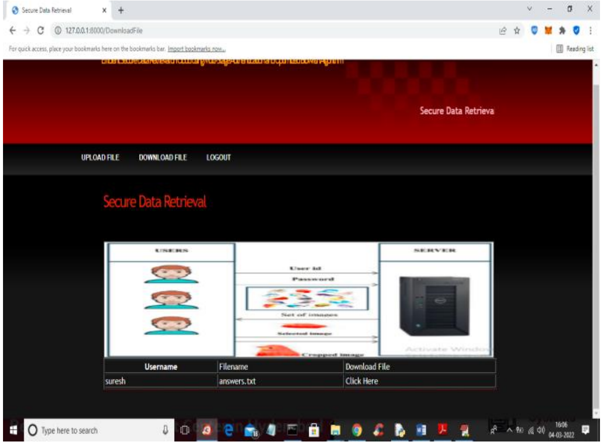
Upload File Screen

Browse File: Choose File No file chosen

In above screen we can see file saved in server static folder and in that file we can see files saved in Blow fish encrypted format like below screen


This PC › Local Disk (E:) › venkat › 2021 › Feb22 › MultistageCloud › CloudApp › static › files
answers.txt - Notepad
answers.txt
1 item 1 item selected 2.61 KB

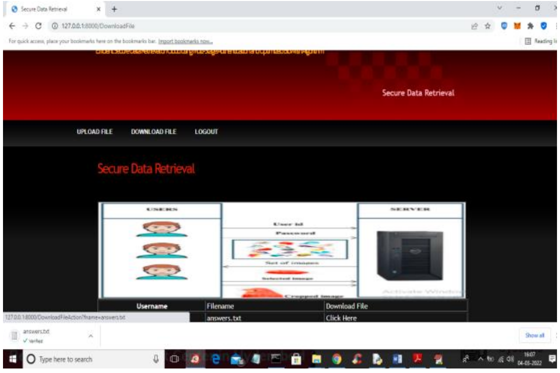
In above screen we can see file saved in encrypted format and now click on 'Download File' link in output screen to get below screen



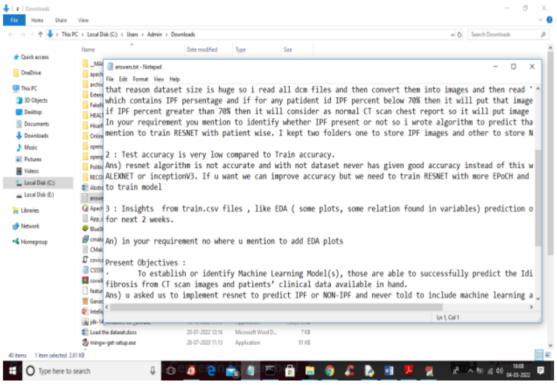
Username	Filename	Download File
suresh	answers.txt	Click Here

In above screen in table we can see all files uploaded by user and then click on

'Click Here' link to download that file in decrypted format



In above screen in browser status bar we can see file downloaded and now open that file to view decrypt ed content


Downloads
This PC > Local Disk (C:) > Users > Admin > Downloads
Name
Date modified
Type
Size
answers.txt - Notepad
File Edit Format View Help
Ln 1, Col 1
Load the dataset.docx 20-01-2022 12:16 Microsoft Word D... 7 KB
mingw-get-setup.exe 28-07-2020 11:13 Application 91 KB
Type here to search

```
that reason dataset size is huge so i read all dcm files and then convert them into images and then read '
which contains IPF persentage and if for any patident id IPF percent below 70% then it will put that image
if IPF percent greater than 70% then it will consider as normal CT scan chest report so it will put image
In your requirement you mention to identify whether IPF present or not so i wrote algorithm to predict tha
mention to train RESNET with patient wise. I kept two folders one to store IPF images and other to store N

2 : Test accuracy is very low compared to Train accuracy.
Ans) resnet algorithm is not accurate and with not dataset never has given good accuracy instead of this w
ALEXNET or inceptionV3. If u want we can improve accuracy but we need to train RESNET with more EPoCH and
to train model

3 : Insights  from train.csv files , like EDA ( some plots, some relation found in variables) prediction o
for next 2 weeks.

An) in your requirement no where u mention to add EDA plots

Present Objectives :
•       To establish or identify Machine Learning Model(s), those are able to successfully predict the Idi
fibrosis from CT scan images and patients' clinical data available in hand.
Ans) u asked us to implement resnet to predict IPF or NON-IPF and never told to include machine learning a
```

In above screen we can see file is decrypt ed and similarly you can upload and download any number of files

CONCLUSION

It's clear that whereas the use of cloud computing has rapidly developed; cloud computing protection is still considered the main matter in the cloud computing traditional atmosphere. Customers don't need to misplace their private knowledge as a final result of malicious insiders within the cloud. In supplement, the slash of provider availability has initiated many difficulties for a significant quantity of purchasers lately. In addition, data intrusion directs to numerous problems for the customers of cloud computing. In this paper, we have now proposed answers for three most trendy safety threats in cloud storage. We now have confirmed that our approach performs better in decreasing the safety threat on cloud For cloud computing to unfold, customers need to have a high degree of believe in the methods by which provider providers guard their knowledge. This learn proposes a Multi-cloud model for Cloud Computing situated on a Separate Encryption and Decryption service, emphasizing that authorization for the storage and encryption/decryption of user information must be vested with two distinctive carrier providers. On this new model, person knowledge in the Storage provider method is all saved encrypted. Without the decryption key, there is no approach for the provider supplier to access the consumer information. Inside the Encryption/Decryption provider approach there is not any stored consumer data, hence removing the probability that person data probably improperly disclosed.

REFERENCES

[1] Mechanisms to protect data in the open cloud from intel, www.intel.com/opensource/openstack

[2] Cloud security mechanisms for data protection : A survey, International journal of multi media and ubiquitous engineering, vol 9,2014.

[3] Data protection- Aware design for cloud computing, HP labs,2009.

[4] Design and analysis of Data protection as a service for cloud computing, IJCSIT, vol 5 ,2014.

[5] Data security and privacy in cloud computing , Hindawi Publishing Corporation, IJDSN, 2014.

[6] Securing sensitive data for cloud computing from IBM,2013.

[7] A secure frame work for cloud computing with multi cloud service providers, IOSR-JCE vol 17,2015.

[8] Bechtolsheim , A. "Cloud Computing and Cloud Networking." talk at UC Berkeley, December 2008

[9] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.

[10] "Cloud security An enterprise perspective" Hewlett-Packard Development Company, L.P. The information, 2012. Available from https://h30613.www3.hp.com/media/files/.../BB237 _Nielson.pdf

[11] O.P. Verma, "Performance analysis of data Encryption Algorithm", IEEE 3rd International Conference on Electronics Computer Technology (ICECT), vol.5, April 2011, pp. 399-403.