INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

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

[1] Mrs. S. YAMUNA , [2] B.MOSHE,[3] D.PAVAN, [4] B.VASANTH

[1.] Assistant Professor Department of Computer Science and Engineering, Teegala Krishna Reddy Engineering College, Rangareddy (TS).India.

Email-:[1.] sarvigariyamunareddy@gmail.com

[2,3,4.]B.Tech StudentstDepartment of Computer Science and Engineering, Teegala Krishna Reddy Engineering College, Rangareddy (TS).India.

*Email-[2]*Moshaybanoth27@gmail.com, [3.] Dongaripavan99@gmail.com

[4.] banothvasanth2000@gmail.com.

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 blowfsh 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, un-authorized person to attack the data. The performance of the proposed methodology is implemented in Python and

ISSN: 2057-5688

performances are analyzed in terms of different metrics.

KEYWORDS: Cloud Computing, Blowfish, Python, Multi-Stage Authentication.

1. 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 iCloud 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.

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 (Sundara Kumar 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 metaheuristics 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.

2. 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 different metrics. In Sudhakar and Rao (2020), Sudhakar et al. had developed a secure aware data transaction on the cloud using an index based quasi–identifier approach. Here, they utilized an incremental and distributed data set for experimentation. Here, initially, input data are clustered with the help of modifed 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 Packetization**.**

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.

3. EXISTING SYSTEM:

Demonstrates the adopted secure routing in IoT-based WSN. The IoT-based WSN is an innovator scheme for smart monitoring. This allows the development of grid sharing for maintaining power quality. The IoT data transfer is done via the Thingspeak application. Thingspeak is a web-based open (API) IoT source information platform that can store sensor data from a variety of ‘‘IoT applications’’ and display it in graphical form on the web. Thingspeak communicates with the host microcontroller via an internet connection that acts as a ‘‘data packet’’ carrier between the connected ‘‘things’’ and the Thingspeak cloud, which retrieves, saves/stores, analyses, observes, and works on the sensed data from the associated sensor to the host microcontroller.

DISADVANTAGES OF EXISTING SYSTEM:

1) Less accuracy

2)low Efficiency

4. PROPOSED SYSTEM:

The existing MHBO model [21] reveals optimal solutions; however, it endures from low precision. To overcome the disadvantages of traditional MHBO, certain improvements are taken, in proposed system we use multi-stage Authentication to secure the data in cloud.

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 blowfsh, 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.

ADVANTAGES OF PROPOSED SYSTEM:

1) High accuracy

2)High efficiency.

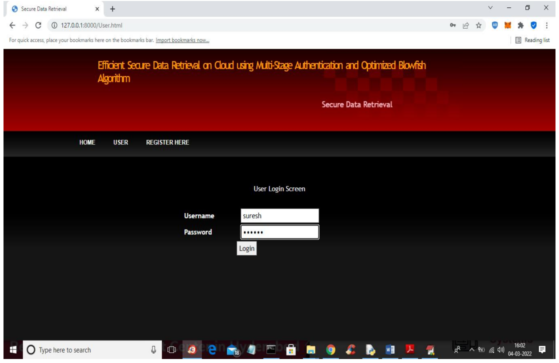
5. MODULES:

Blowfish 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.

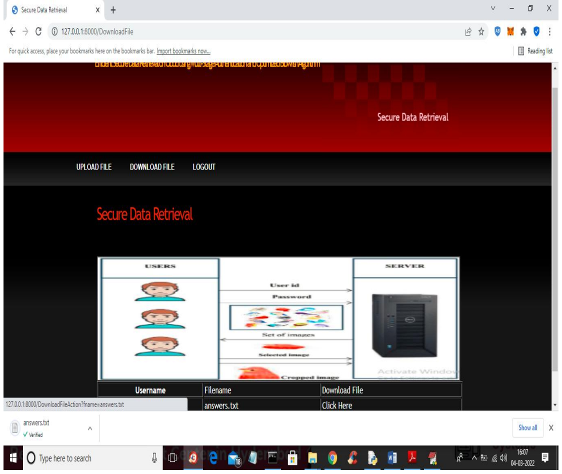
While login multi authentication is applied by asking user to enter username and password and if login successful then display list of images and user has to select correct image given at registration and if correct image is selected then only allow user to upload and download filet

6. RESULTS:

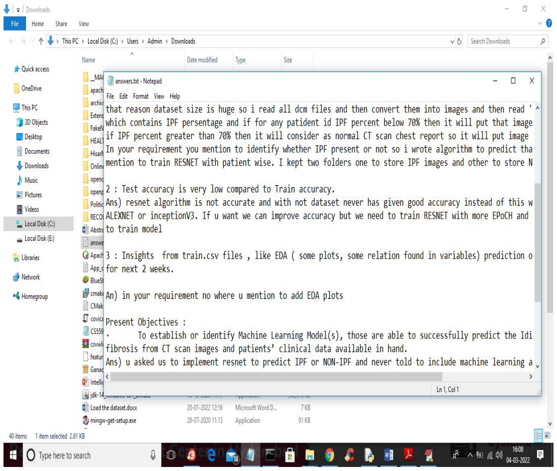

Secure Data Retrieval
127.0.0.1:8000/User.html
Efficient Secure Data Retrieval on Cloud using Multi-Stage Authentication and Optimized Blowfish Algorithm
Secure Data Retrieval
HOME
USER
REGISTER HERE
Login

User Login Screen

Username: suresh
Password: ••••••



Username	Filename	Download File
	answers.txt	Click Here



```
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
```

7. CONCLUSION

In this paper, a secure aware data transaction on the cloud has been explained. Here, user authentication verification is an important task that has been explained. Here, the data has been encrypted using the OBA algorithm. The BA has been enhanced using the BCSO algorithm. The mathematical expression of both the algorithm has been explained. Using this method, we can avoid the unauthorized user login process. The performance of the proposed methodology has been analyzed in terms of diferent metrics namely, encryption time, decryption time, file access time and memory. Our suggested technique has less encryption and decryption time than the current technique, as shown by experimental outcomes. Hence our proposed method is highly preferable than the existing methods. The user cannot retrieve the file without authentication verification hence this method is highly secured. In future efficient algorithms could be used for increasing the speed of the overall process.

8. REFERENCES

[1] Bai TDP, Raj KM, Rabara SA (2017) Elliptic curve cryptography-based security framework for internet of things (IoT) enabled smart card. In: 2017 World congress on computing and communication technologies (WCCCT) IEEE, pp 43–46

[2]. Brindha T, Shaji RS (2018) A secure transaction of cloud data using conditional source trust attributes encryption mechanism. Soft Comput 22(3):1013–1022

[3]. Burger PM (2001) Biometric authentication system. U.S. Patent 6(219): 439

[4]. Cheng H, Rong C, Qian M, Wang W (2018) Accountable Privacy preserving mechanism for cloud computing based on identity based encryption. IEEE Access 6:37869–37882

[5]. De la Prieta F, Rodríguez-González S, Chamoso P, Corchado JM, Bajo J (2019) Survey of agent-based cloud computing applications. Future Gener Comput Syst 100:223–236..