IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Efficient Secure Data Retrieval On Cloud Using Multi-Stage Authentication And Optimized Blowfish Algorithm

Mohd Yousuf[1] , Sridhar Gummalla[2] , Shaik Shakeer Basha[3]

[1]PG Scholar, Department of Information Technology, Shadan College of Engineering and Technology, Hyderabad,

[2]Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology,

[3]Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology,

ABSTRACT - Cloud computing has matured, and a diverse range of cloud service providers are available. Security issues continue to receive a lot of attention. Concerns regarding privacy and security frequently pose a serious obstacle to users' acceptance of cloud computing methods and the benefits they provide over earlier systems. In a cloud-based setting, biometric technologies can present some challenges related to the administration of biometric data because of privacy laws and the requirement to trust cloud providers. Biometric methods are increasingly the core component of a wide range of guarantee identification as well as private identification solutions. In this research, we present a crypto biometric solution for computing in the cloud that solves those issues without exposing any private biometric data.

OBJECTIVE:

Even contractual arrangements involving vendors and users addressing security are currently lacking. Our investigation focuses on acceptable security measures that might perhaps satisfy conventional legal standards. Biometrics have undergone much research in the past decade, and their applicability to security have grown increasingly clear. Combining cloud computing with biometric technologies creates fresh research and application possibilities for cloud user data security.

INTRODUCTION

1.1 INTRODUCTION

A fresh type of company and trend in the architecture of applications are both cloud computing. The concept has shown to be applicable to a wide range of solutions, encompassing the multiple tiers described in the cloud architecture (SaaS, PaaS, and IaaS), as seen by the success of numerous suppliers of services, with Amazon serving as a notable example. Although there are still some restrictions and difficulties, we can say that the use of cloud computing is at a mature stage. For businesses that outsource their infrastructure, apps, and data, cloud computing offers significant advantages at the expense of data management. Computers not owned, operated, or managed by the users process the data. In this situation, the user is unaware of how the supplier manages the data, therefore A lot of confidence is required. The absence of control over the structure's logical and physical components forces significant adjustments to security and privacy practices. Even contractual arrangements between service suppliers and users regarding security are currently lacking. Our

research emphasizes acceptable security measures that might perhaps satisfy standard legal standards. Biometrics have undergone numerous studies in the past decade, and their applicability to security have grown increasingly clear. The fusion of biometric technologies with cloud computing creates fresh research and application prospects for cloud data security. Given that biometric data is sensitive to privacy, even cloud service providers must maintain the security of biometric templates Due to the difficulty of altering information about users in the same manner as numerical passwords, this requirement is particularly crucial. Cloud computing has matured, and a diverse range of cloud providers are available. Security issues continue to receive a lot of attention. Security and privacy concerns frequently pose a serious obstacle to users' acceptance of cloud computing systems and the benefits they provide over earlier systems. In a cloud-based setting, biometric technologies present some challenges related to the administration of biometric data because of privacy laws and the requirement to trust service providers. Biometric devices are increasingly the core component of a wide range of secure verification as well as private verification solutions. In this research, we offer a crypto biometric approach for cloud computing that addresses those issues without exposing any personal biometric information.

2. LITERATURE SURVEY

In order to address security issues with online computing, the key relation approach that is now in use must be improved. By evaluating the results of the experiments, they also demonstrated that the CA converter and shifter, used for encryption and decryption, respectively, aid in reducing time complexity and cope with different security assaults more effectively. A combination cryptographic method combining the public RSA cryptosystem with knapsack has been suggested by author Fadhil. The suggested method is less complicated and more secure than a single algorithm. It operates in two steps: it performs RSA encryption, which first, then sends the output to the knapsack technique. When performing the decryption procedure at the receiver end, the opposite procedure must be used.

Based on Grey Level the Combination The matrices (GLCM), which describe the s true-patronship between neighboring pixels, the Grey Level The Combination Matrices (GLCM) approach [8] was developed. From each GLCM matrix, fourteen characteristics are extracted, including the maximum Pearson correlation coefficient, the angle of the minute moment, comparison, relationship, variance, the opposite difference period, summarize average, total variance, sum the entropy distinction variance, and distinction entropy.

The authors Chen and Shuckers [6] distinguished the two methods: the optical fingerprint camera with the group classification approach in addition to the wavelet-based detection of life method. For assist occurrences and energy signatures that are generated they developed energy fingerprints. The topic of processing noisy data for biometric detection is covered by Zhifan Gao et al. [7]. They looked at the region of interest utilizing graphic pixels as a fingerprint and a pattern. Additionally, they use the FVC2002 dataset to successfully obtain the EER of 5.6% from 3.5%. Zin The filtering with Gabor approaches are suggested by Mar Win et al. [8] for gathering the fingerprint characteristics. A greater accuracy of 97% is recorded when the current approach is compared to the current methodology. Zhu Le-Qing [9] researches the robust quickened-up knuckle print identification system has an algorithm. The test findings also demonstrate an excellent precision of 96.91% and a relatively short calculation time to match the finger prints for authentication.

The test for fingerprinting evaluation was carried out by Jucheng Yang et al. [10] with the aid of the current by FVC2002 dataset that had been put together. For fingerprint mismatch detection, they achieved a faster execution time and an EER of 2.27%. A number of techniques to identify fingerprinting from the scanner were introduced by Nika and Agarwal. Additionally, the wavelet transform technique is used with the neighborhood binary pattern approach to detect fingerprints. However, this technique is used to determine whether a fingerprint is genuine or not [11]. Along with other methods like Gabor filter approaches [12], wavelet transformation [13], and curvelet grow [14], there is an additional approach called Grey Level the Combination Matrices (GLCMs). For the purpose of implementing a learning method, Nogueira et al. provide fingerprint identification. Principal Component Analysis, or PCA, and Support Vector Machine (SVM)

3. OVERVIEW OF THESYSTEM

3.1 Existing System

Data security issues are described by Chow et al. [2] along with how they affect the adoption of clouds and how current research may help to resolve them. When it comes to managing data access in cloud computing, Hucheng et al. focus on scalability and data privacy in [3], assigning most computationally demanding activities to cloud servers. [4] describes a distributed approach to guarantee the accuracy of user data in the

cloud. Creese et al. [5] look at how data protection controls are designed in a cloud setting. [6] studies the issue of guaranteeing the integrity of stored information in cloud computing and proposes a methodology utilizing third party authority.

3.1.1 Disadvantages of Existing System

Studies the issue of assuring the integrity of information stored in cloud computing and proposes a methodology utilizing third party authority. It's yet unknown what drawbacks this intricacy could cause. Depending on the subsystem to be protected, many methods can be identified. These problems are discussed in "Cloud Protection Issues" [1], which also specifies a SLA to characterize various security levels.

3.2 Proposed System

For each user that registers with the application, a biometric database is used in the suggested system, and its biometric information is trained using the CNN algorithm. The model's accuracy is determined, and the trained model is applied in the cloud setting to perform user data such as fingerprints authentication. When a user registers with a website, user uploads a finger print to be compared to a model; if the two match, login is effective; if not, authentication is unsuccessful.

Advantages of Proposed System

✓ This method helps in effective management of user authentication with both passwords based in finger print authentication,

✓ This process automates authentication mechanism using Deep learning.

3.3 Proposed System Design

In this project work, I used five modules and each module has own functions, such as:

1. Dataset
2. Preprocessing
3. Segmentation
4. Classification

3.3.1 *Dataset*

Dataset of different users' fingerprint is converted in to image format and used as dataset. There is not specific limit of user dataset for this project four user's dataset is collected and taken as input which has features as images and labels as username.

3.3.2 *preprocessing*

Pre-processing is a technique used to improve image quality and boost visualization. Image processing is an important aspect in medical imaging that helps to enhance picture quality. This might be one of the most important variables in attaining good outcomes and accuracy in the next phases of the suggested technique. Finger print images may have a separate problem that causes poor and low visualization. If the photos are inadequate or of poor quality, the outcomes may be disappointing. During the preprocessing stage.

3.3.3 Split data

We have now separated our dataset into the testing and training halves. The sole purpose of this split is to gauge how well our model has extended in terms of learning method and to assess our accuracy on fresh dataset. Model fitting, a crucial stage in the model development process.

3.3.4 *Classification:*

The suggested CNN structure consists of numerous layers, beginning with the input layer, which contains the augmented pictures from the previous pre-processing phase, and progressing through the convolution layers and their activation functions, which are utilized in feature selection and down-sampling. A dropout layer is used to prevent overfitting, followed by a fully connected layer and a SoftMax layer to anticipate the output, and lastly a classification layer that outputs the predicted class.

3.3.5 Owner Module:

The trained CNN model is used to confirm owner logon. Owners may connect to the program using his username and password after registering with all the required information. Once logged in, he can upload files to the cloud and share them with other users who have already registered. He may also access the files that he has posted, as well as other users' requests for secret keys, to which we can answer by sending the user the key via mail. He may examine the information and download the file using that blowfish key

3.3.6 User Module:

The user receives a user name and password after registering with the program. The keys for blowfish are sent to the owner email address and may be used for the owner download. The owner can access all encrypted files submitted by all users, send requests to the appropriate users, and get authorization to download data.

4 Architecture

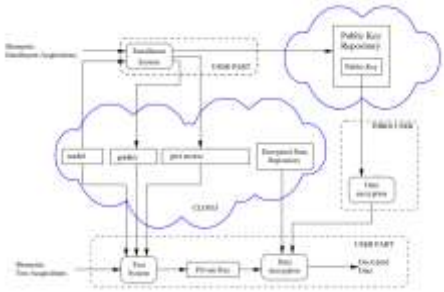

Fig 1: Frame work of biometric recognition

5 RESULTS SCREEN SHOTS

Home page with upload and view features

View encrypted data with key generation

View data with download options

Send request page for key request

6. CONCLUSION

The fundamental objective is to safely store, authenticate yourself and access data in a public cloud that is not within the data proprietor's control. To secure data files in the cloud, we use the Blowfish cryptographic encryption method. The cloud server's authentication increased the speed of data access and storage. Another benefit of using methods of encryption is that they enhance performance throughout the encryption and decryption processes. We believe that this method of data access and storage is highly efficient and safe. We are working to use a single data encryption technique in a cloud-based computing setting to tackle the security problems problem. The CNN method is employed to gather and train individual finger print data, and the learned model is subsequently used for verification.

Future Enhancement

For security reasons, the suggested system encrypts data using three different methods, as seen in the cloud environment. In the future, a multi-dimensional program may be created that allows users to choose from two or three different encryption techniques for each file they upload, giving each one a unique set of security measures.

References

[1] Peter Mel and Tim Grace, "The NIST Definition of Cloud Computing", NIST, 2010.

[1][2]Achill Buhl, "Rising Security Challenges in Cloud Computing", in Proc. of World Congress on Information and correspondence Technologies ,pp. 217-222, Dec. 2011.

[2][3]Srinivasarao D et al., "Breaking down the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011

[3][4] Tingyuan Nye and Tang Zhang "An investigation of DES and Blowfish encryption algorithm‟ , in Proc. IEEE Region 10 Conference, pp. 1-4 ,Jan. 2009.

[4][5] Jitendra Singh Adam et al.," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" , International Journal of Advanced Research in Computer Science and Software Engineering ,vol. 2,Aug. 2012.

[5][6] Manikandan.G et al., "A changed cryptographic plan improving information", Journal of Theoretical and Applied Information Technology, vol. 35, no.2, Jan. 2012.

[6][7] Niles Maintain and Subhead Bhingarkar, " The examination and Judgment of Nimbus, Open Nebula

and Eucalyptus", International Journal of Computational Biology , vol. 3, issue 1, pp 44-47, 2012.

[7]Sinkov A., "Elementary Cryptanalysis – A Mathematical Approach", Mathematical Association of America, 1996

[8]L. Arockiam, S. Monikandan "Data Security and Privacy in Cloud Storage using Hybrid Symmetirc Encryption Algorithm", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, pp 3064-3070, August 2013.

[9]G.L.Prakash, M.Prateek and I.Singh, 'Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System', International Journal of Engineering and Computer Science, Vol. 3, Issue 4, April 2014, pp. 5215-5223.

[10] [5] Juels, Ari and Burton S.Kaliski Jr. 'PROs: Proofs of retrievability for Large Files', Procedding of the 14th conference on Computer and communication security, ACM 2007.

[11] [6] Fadhil Salman Abed, "A Proposed Method of Information hiding based on Hybrid Cryptography and Seganography", International Journal of Application or Innovation in Engineering & Management, Vol. 2, Issue 4, April 2013.