ISSN: 0974-5823 Vol. 7 No. 2 February, 2022

International Journal of Mechanical Engineering

FACIAL GEOMETRIC KEY BASED HOMOMORPHIC CLOUD SECURITY USING NEURAL NETWORK OPTIMIZATION

TADI. CHANDRASEKHAR

ECE Department, ISTS Women's Engineering College, Rajahmundry, India.

CH. SUMANTH KUMAR

ECE Department, GITAM University, Visakhapatnam, India.

ABSTRACT

Cloud computing has been an intergral part of the technological and personal interaction with the computing devices in current times. The cloud service that are in utility are providing users with legacy protocol for the authenticaction of the device, most of the cloud platforms use traditional encryption procedures for the authenticaction of the devices. This paper present a facial authenticaction protocol that will create a facial geometric point as a key for the encryption process. The procedure was developed as a multi stage implementation of the interacting facial recognition algorithms. The first sequence of the algorithm is implemented on the basis of fuzzy neuro inference algorithm which implemented the facial authenticaction of the users and making an entry of the individual into a sheet tracking. The second procedure used a Convolution neural network (CNN) with VGG19 based architecture for facial geometric point mapping of a face for recognition of deep facial features. Based on the algorithm a facial geometric point based facial network was developed and individual faces and labelled.The procedure also introduced a multiple face recognition in a single image.Thes third procedure uses a facial geometric point recognition based cloud authentication system.This system creates a dynamic encryption key which is based on facial geometric points that will be given as input to the encryption cipher.These facial geometric points which are calculated based on the number of regions that were detected on an individual face each point is then dynamically assigned a value and given as an input to the key of the individual algorithm so the file is encrypted, these geometric points will also used for the decryption of the file.

Keywords: *CNN, Encryption, Geometric points, Fuzzy neuro System.*

INTRODUCTION

The field of biometrics incorporates constant facial acknowledgment. Biometrics alludes to a PC's ability to recognize an individual in light of an extraordinary real trademark. Face acknowledgment is the limit with regards to a PC to perceive an individual in view of their facial elements. Biometrics is becoming one of the most quickly growing areas in trend setting innovation. Biometrics are relied upon to detonate in the following century to validate personalities [10] and forestall illicit admittance to organizations, information bases, and offices, as per forecasts. A facial acknowledgment gadget is a device that matches a picture or video of a human face to other picture faces put away in an information base.During the face ID processes, the construction, shape, and extents of the appearances are thought about. Additionally, thought about are the distances between the eyes, nose[8], mouth, and jaw, the top shapes of the eye attachments, the sides of the mouth, the arrangement of the nose and eyes, and the district encompassing the actually take a look at bones. A few pictures of the subject should be taken at various points and with shifted looks while using a face acknowledgment program. The singular stands before the camera for a couple of moments during confirmation and recognizable proof, and afterward the picture is contrasted with those recently recorded [9]. On account of its benefits, facial acknowledgment is oftentimes used. The advantages of face acknowledgment incorporate the way that it is non-meddlesome and might be performed from a remote place without the subject staying alert that the person is being filtered. Face acknowledgment frameworks are better than other biometric approaches in that they might be utilized for observation reasons, for example, looking for needed lawbreakers, suspected fear-based oppressors, or missing kids. Face acknowledgment advancements are more helpful for facial verification than for distinguishing proof [11] since it is not difficult to transform somebody's face and a cover might be utilized to conceal the person. The climate, just as subject developments and camera center, are generally factors to consider. At the point when utilized related to another biometric innovation, facial acknowledgment may radically improve confirmation and recognizable proof results. Scientists in the areas of safety, brain research, and picture handling are totally intrigued by face acknowledgment. It considers a huge report field. The utilization of facial acknowledgment to help law requirement is a significant application. The programmed recovery of suspect pictures from the police mug-shot information base can help officials in quickly reducing imminent suspects. Face acknowledgment applications require a constant reaction, and executing it on a cell phone gives portability since it is available from anyplace. Without fail, the endeavored arrangements fill in intricacy and execution times, however they remain amazingly hard to carry out in cell phones' assets like energy [12], handling power, and information stockpiling. Since it moves figuring power and information stockpiling away from cell phones and into the cloud, versatile distributed computing tackles the cell phone asset

challenges that fundamentally obstruct the improvement of administration quality. It brings applications and versatile registering to a lot more extensive scope of portable supporters, bringing applications and portable figuring to cell phone clients as well as a lot more extensive scope of portable endorsers. Because of Mobile Cloud Computing [13], clients will actually want to get to a plenty of new elements that will upgrade their telephones. A concentrated observing and upkeep of programming in the cloud has worked on the security of cell phones.

In this paper we look at the face recognition techniques. We categorized the techniques under three categories namely holistic, feature based and hybrid approaches

The major contribution of this paper:

• Highlight various algorithms used for facial recognition

• Deep facial features recognition using Neural networks

• Evaluation of Deep Facial Homomorphic Encryption.

RELATED WORK

Numerous analysts have chipped away at design acknowledgment and recognizable proof through different biometrics using different developing mining model philosophies because of the significant development of AI, the PC climate, and acknowledgment frameworks. [1] proposed a clever way to deal with move figuring out how to programmed feeling acknowledgment across different modalities [3] proposed an original way to deal with move figuring out how to programmed feeling acknowledgment across different modalities [proposed an original way to deal with move figuring out how to programmed feeling acknowledgment across different modalities [4] proposed an original way to deal with move figuring out how to programmed feeling acknowledgment across different Saliency maps are utilized in the proposed model for look recognizable proof to send information from a self-assertive source to an objective organization by basically "stowing away" non-important data.Since the experience is just imparted through increase of the info information, the recommended method is free of the model utilized. At the point when the proposed model was pushed to zero in on the pieces of the info that were respected significant sources, the evaluation uncovered that the new model had the option to adjust to the new area quicker. [2] proposed a programmed facial acknowledgment framework in light of an exchange learning technique and a Convolutional Neural Network. CNN utilizing loads gained from the VGG-16 pre-prepared model. To accomplish face acknowledgment, the Archive Face [3] recommended added substance precise edge misfortune. Because of the exact connection to geodesic division on a hypersphere, the recommended Archive Face has an undeniable mathematical cognizance.They likewise introduced the most thorough exploratory assessment of the FR approach utilizing ten Face Recognition datasets. They asserted that Archive Face reliably beats the opposition and can be carried out with negligible processing cost. On the Labelled Face Wavelets, Center Abled Face Wavelets, and Counter Point Labeled Face datasets, the confirmation execution of open-source Face Recognition models was 99.82 percent, 95.45 percent, and 92.08 percent, separately. [5] Space express data advancement was introduced to develop arranged data sizes for face affirmation systems. They showed how to work on sensible datasets with key facial varieties by dealing with the countenances in the datasets and utilizing common convolutional neural nets to arrange request photos. They put their framework under serious scrutiny by running it through the labelled Faces benchmarks and Janus on countless downloaded pictures. They expressed a mean gathering accuracy of 100% equivalent mistake rate and announced the traditional show for unhindered, set apart external data. [7] Fostered a key administration framework before cutting edge secret sharing. The objective of this work is to give a more dependable decentralized light weight key administration approach for cloud frameworks that will further develop information security and key administration [14]. The recommended arrangement safeguards the security and protection of client information by imitating key offers across many mists using a mystery sharing instrument and a democratic technique to confirm share respectability. The methodology utilized in this concentrate likewise further develops protection from byzantine disappointment, server intrigue, and information modification assaults.

METHODOLOGY

The methodology follows the various procedural elements initially the fuzzy neuro inference networks were used to implement the facial security of the users the dataset used here is YALE and ORL dataset. The second procedure used was facial geometric points of the same dataset to extract the deep facial features the algorithm used is CNN (Convolution Neural Networks) with VGG19 network. The facial geometric points are used for the facial recognition of the celebrities by using Deep Facial Feature Training of the VGG16 network the custom network of 100k samples were processed. Multiple facial feature recognition for the celebrities with facial labelling was developed with deep labelling techniques. The final phase implemented the facial geometric points for the cloud computing security during the authentication and encryption phase. This phase implemented a facial cloud weblog in which used a camera-based login portal. The authentication system will consists of the collection of the facial samples which constitutes of the training phase and then the cloud login portal used as the testing phase. Then facial geometric points were used to encrypt the files with the random facial points extracted from the phase.

Figure: ORL dataset images

Figure: Yale-B dataset images

3.1Fuzzy Neuro Inference Network Based Automated Facial Recognition:

A *fuzzy neural network* is a structure FNN (*U*, **W, X, Y**, *L*) with the following specifications:

a) *U* is Sample container of the facial template for Fuzzy Neurons.
b) The image parametersof the fuzzy neural network are designated with the corresponding weight matrix **W**given by matrix product $U \times U \rightarrow D_W$ (D_W weights of the facial features).
c) The image vector inputs $\mathbf{X} \in D_X$ describes as the input image maps (D_X is domain of input maps).
d) The image vector outputs $\mathbf{Y} \in D_Y$describes as the output image maps (D_Y is the domain of the output vector).
e) The learning algorithm *L*will be trained for the images given to input and output maps

Fuzzy neural networks, are based upon fuzzy logic operations, while others lack some of the fundamental structural characteristics of neurons.The training images are first given to the input neurons, each image with its corresponding facial features are treated as nodes that constituted training. Thefacial feature neuron and its derivatives are stored as processing units that are fundamentally stored.The facial features units that are stored are formed as fuzzy network then each image is then tested on basis of the facial neuron of that are trained to the network.

3.2Facial Geometric Points Using CNN

The facial Geometric points are based on the three-phase setup of the Convolution neural network structure

1. Face Detection

2. Recognition Mode

3. Face Tracking

Face Detection

Face Detection is a basic functionality in facial geometric points detection. The facial detection calculation is based on the micro-resolution that are divided by the Convolution Neural Networks. When each face sample that is processed through the procedure for the assemblage images, these images are formed as picture pyramid based on the various micro resolutions these Convolutions layers (used only 3*3 size), Max pooling layers (used only 2*2 size)and Fully connected layers at end for face detection and arrangement. Regardless of whether the picture is face or non-facial, the gathering characterizes it. Before the acknowledgment stage, the total recognizing face picture is contracted to 160x160 pixels.

Recognition Module

Facial recognition dependent on the neural networks is designed based on the network layers that are designed by the Convolution Neural Networks this is a high-performance computing. This methodology of the is based on the VGG16. Accordingly, we utilized a VGG16-put together face acknowledgment approach based with respect to Inception engineering, in which we save the layers of the countenances recognized in a mat record and a h5 document for acknowledgment. The point is to diminish the information picture's inserting in a similar individual's component space while expanding the essence of an alternate individual to be far away. A facial key marker is additionally proposed here for recognizing a particular part of a face in a given picture with the posture of the individual characterized in the shot. We moreover make a xml document in the location stage that contains the name of the connected face.

Adaptive Face Tracking

In light of the cycles of every progression, like face location, face plan, and face acknowledgment itself, the planning time is the vital worry in face acknowledgment system for present application. Face recognition consumes a ton of handling time for each situation in our trials when we applied it to the entire image of each edge in the photograph. At the point when a face is noticed, we anticipate that it should stay in the scene for a brief time frame.We utilized calculation to follow the face involving a relationship channel that was subject to estimation thusly. The perceived face from the h5 and mat documents is then contrasted with the xml records to see whether a face can be connected to a document name. The key markers are then coordinated to a particular region of a face that has the attributes.

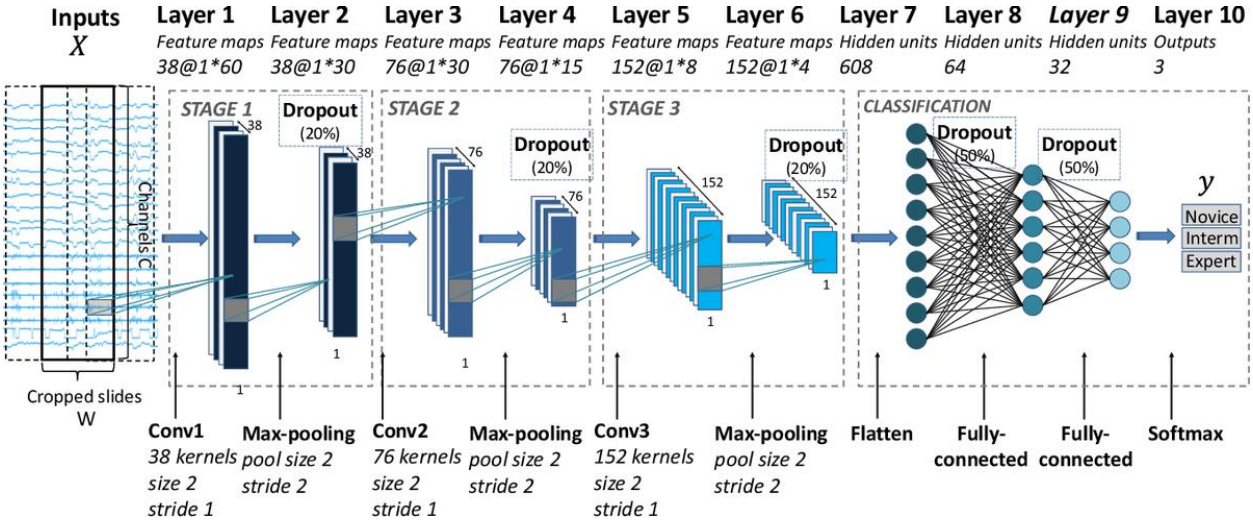

Figure: Applications of facial key markers using CNN

In every one of these models, the inability to plan data was referred to as a critical hindrance to creating sound models. Subsequently, some went to bigger 3D item instructive records or misleadingly created models. We offer a substantially more simple other option and show how it may bring about solid repeat of different task and application names in paper titles connecting with two of the most notable key terms.

AUTHENTICATION ON CLOUD

In this arrangement, there is likewise a cloud server. This reflection depends on a Network Attached Storage server, which might be sent on an assortment of equipment stages and consumes little assets. The record is consequently divided, and the solicitation is shipped off the homomorphic encryption strategy. The strategy starts with the camera input for the face test, which fills in as the key for the record's encryption. From that point onward, the record is handled and shipped off the cloud server's stockpiling. The client is incited with face input during the recovery methodologyas key in decryption of the file.

Algorithms

4.1.Fuzzy Neuro System

A fuzzy neural network implements the neurons on facial sample using fuzzy logic in many Different areas, including the info yield level, neurotransmitters, the conjunction cycle, and surprisingly the initiation work We'll utilize the language utilized in x is the fluffy information vector and y is the fluffy result vector, the two of which are fluffy whole numbers or stretches, to create an exact numerical depiction of the fluffy neural organization. W represents the association weight vector. From the n-layered info space to the l-layered space, we might characterize the accompanying planning numerically:

$x(t) \in Rn \rightarrow y(t) \in Rl$

The likeness between the fluffy information vector x(n) and the association weight vector not entirely set in stone by a conjunction activity (n). The juncture activity portrays a summation or item activity in neural organizations, though it characterizes a number juggling activity in fluffy neural organizations, like fluffy expansion and fluffy augmentation.

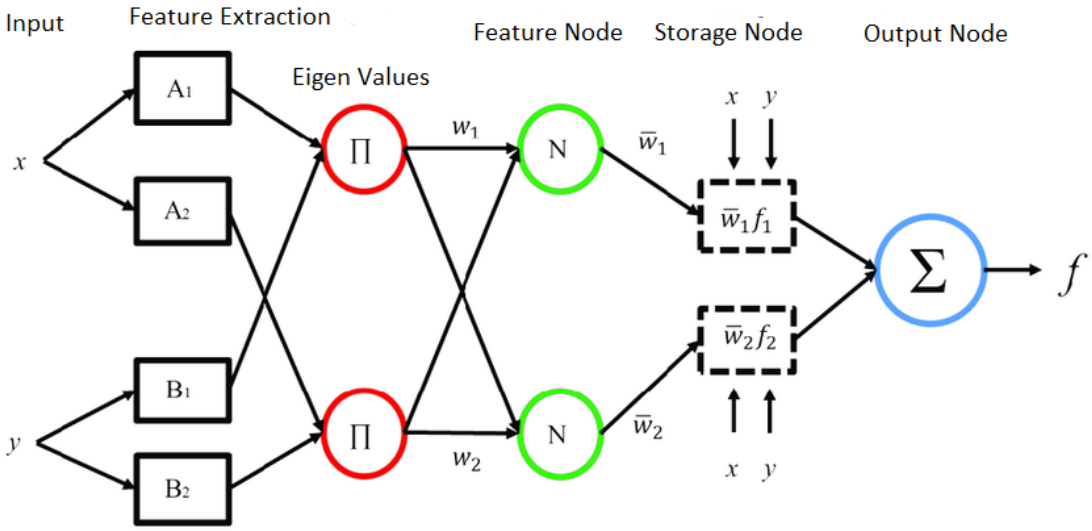

Figure: Fuzzy Neuro System Block Illustration

The output neurons implement the following nonlinear operation:

(z(n)=ψ[W(n)⊗x(t)]Based on the given training data {(x(n),d(n),x(n)∈Rn,d(n)∈Rl,t=1,…,N} the cost function can be optimized:

EN=∑n=1Nd(y(n),d(n))

where d(·) defines a distance in Rl.The learning algorithm of the fuzzy neural network is given byW(n+1)=W(n)+∈ΔW(n)nd thus adjusts NW connection weights of the fuzzy neural network.

4.2Convolution Neural Networks

The sample collection phase denoted by $€^{\mu}_{e,k}$, $c^{\mu}_{i,p}$.Each sample is collected and indexed with {e,k} p and k $h^{u}_{j,q}$. The subsequent neurons are interconnected and were being assigned weights

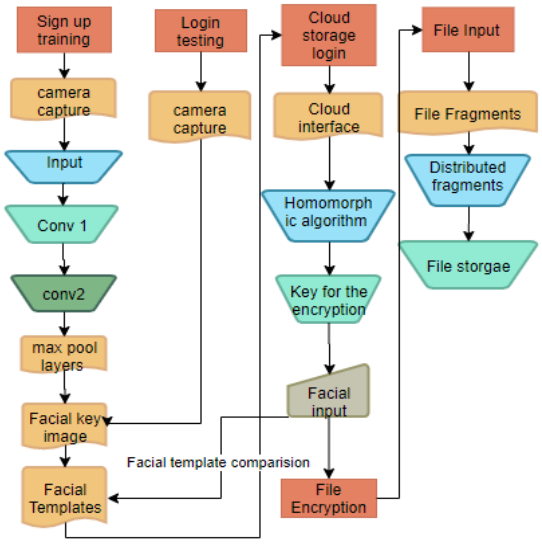

Figure:The Architecture of the facial key based cloud storage

$w^{q}_{j,s}$, q= {-Q, …,0, …, Q} connected by the filter $€^{\mu}_{e,r}$. Convolution Layer μ and corresponding parameters t, swill obtain n inputs from users

$g^{\mu}_{y\,q}=\sum W \sum R w^{t}_{i,j} €^{\mu}_{,q+t} + b_x$

$€^{\mu}_{j}$is the translation vector and the position is set to q, by setting r= q + t. The hidden features of the pixel array of the hidden layers and denoted by

$V^{u}_{j,q} = g(h^{u}_{j,q})$.

The change in the resolution for the max pooling layer with change in the micro resolution parameter for the sample is $\Delta T^{d}_{j,k}$ is the processed image with medium resolution.

$$\Delta T^{d}_{j,k} = \acute{\eta}\, \Sigma_{\mu,r}\, \delta^{\mu}_{j,r}\, €^{\mu}_{l,q+t}$$

Where$\delta^{\mu} J_{j,q}$is the image with the higher resolution

$$\delta^{\mu} J_{j,q} = \Sigma_{t} F^{|}(g^{\mu}_{j,q}) \sum_{l} \delta^{\mu}_{i,q-s} v^{s}_{i,j}.$$

The RELU layer of the CNN with the indexing parameter with all the patters that processed through the system is defined by the following equation.

$$\delta^{\mu} K_{i,p} = [e^{\mu}_{i,p} - p(h^{\mu}_{i,p})]\, e^{|}(d^{\mu}_{i,p}).$$

The parameter k is given as the input to fully connected layer $\{\delta^{\mu} I_{j,q,\Delta} I^{d}_{j}, \delta^{\mu} I_{i,p}\} = \{\delta^{\mu} I^{|}_{j,q,\Delta} I^{|d}_{j}$and $_{\delta}{}^{\mu} I^{|}_{i,p}\}$ where $I^{|}$is the image sent to the output layer. The indexing parameter values of s= {-S...,0 …, S}, and 2S+1 are defined as the filter length of the output layer and the output layer is defined as

$$O^{\mu}_{i,p} = f(i^{\mu}_{j,p}) = h(\sum K \sum T w^{s}_{i,j} U^{\mu}_{j,p+s} + b_{i})$$

Spatial feature weight shifting features for the output layer and the resultant cost function which is defined as

$$F = \frac{1}{2} \Sigma_{\mu,k,q} [D^{\mu}_{i,p} - M^{\mu}_{i,p}]^{2}.$$

The whole process will constitute of the training part of the system and a resultant network file is stored in the root directory of the system. The testing part is defined by the equations .Each image is processed through 4 and 5 equations and be matched with the network file and identified for their subsequent entry if the image is matched then the key points will be formed by equation 6 key points are displayed on facial region.

4.3.Homomorphic Encryptiononthe on cloud

The input file that had homomorphically encrypted through$f \oplus k$and *f* file with key *k. [[f]]=Enc(f, k)=f* $\oplus$ *k* .The encrypted file [[f]] is existing in the storage. The decryption of the exiting file on the cloud storage is defined by *f=Dec([[f]],k)=[[f]]* $\oplus$ *k.* And the key is defined by the following.

$$K = \sum_{g=0}^{m1} \binom{h}{g} \leq \frac{2l}{s} \leq \sum_{i=0}^{m1+1} \binom{h}{g}$$

From the above equation h and g are the facial features of the algorithm and the random keys generated by the algorithm are of 8-bit value and the values of m ranges from m={-m,0….,m}. And the decryption of the fie will be given by the following

$$[f] = \sum_{i=0}^{m1} \binom{h-1}{g} \leq \frac{2l-1}{s} \leq \sum_{i=0}^{m2+1} \binom{2h-1}{g}$$

The files on the server will be existing in the random fragmented format and all these fragments are joined together in multiples.

RESULTS

The Facial Authentication of the cloud computing system follows route by beginning the procedure with Fuzzy neuro System. This system implements the facial neuron channeling of the facial features as discussed above. The methodology uses YALE and ORL datasets for collection of the facial templates from 100k samples. Based on the dataset information the fuzzy neuron was trained and the facial camera samples of the non-dataset users have been collected. There are 1000 users that were used in the training process along with the users from the dataset. Based on the data fuzzy system is used to store neurons in the network of neurons. The testing was conducted on these samples where the accuracy is found to be 92% various other parameters are discussed below.

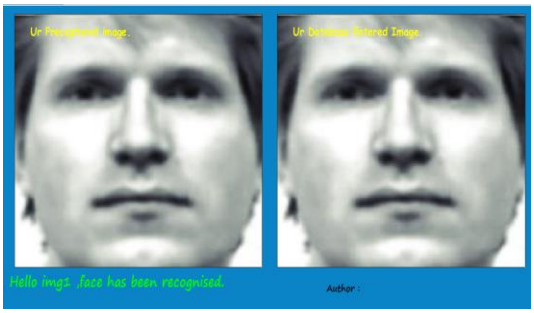

Figure: Fuzzy Neuro System Face Recognition

The Second section of the implementation of the cloud security is developed on the basis of the facial geometric points that are implemented on the same dataset. The CNN algorithm with VGG19 networks has been used to implements the recognition of deep features from the facial templates that provided in the dataset. The facial geometric points are obtained from the deep features

calculated by CNN. The processing is done through various layers of the CNN and the features are stored in the output layer of the algorithm. The facial geometric points are displayed on the face by using calculating the facial geometry which is discussed above.

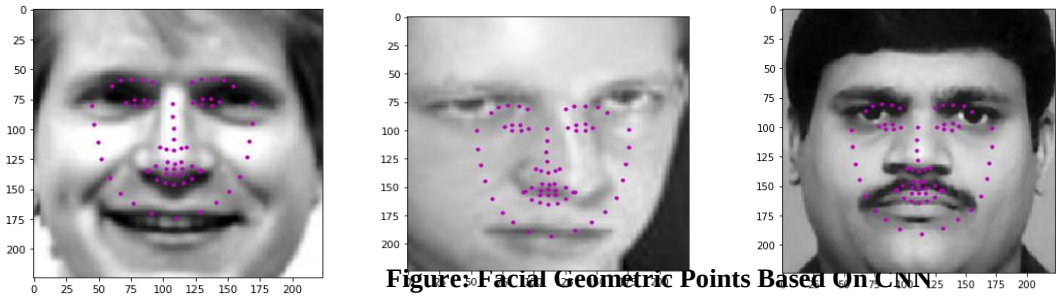

Figure: Facial Geometric Points Based On CNN

Then the system implemented the multi facial recognition of the celebrities from black pink Korean datasets. There are about 200k samples collected in the due process. Each celebrity with their individual face were trained and testing is conducted on the group photographs where each face is labelled facial geometric points have been labelled based on the facial geometry. This facial geometric points procedure is further continued into cloud computing security of the users.

Figure: Multiple Facial Recognition Based on Facial Geometric points

0The facial geometry is calculated on live captured images that were given as input to web-based login for the cloud portal that was developed on flask framework and hosted on the Heroku server. The private cloud server has been developed on the NAS based storage. Each user signup process was prompted with live collection of user samples from the web camera based on the developed algorithm the user's data was stored in the database entries and network log file of CNN. This process constitutes the training process the facial geometry is calculated based on the geometric point that are fetched by the algorithm. These facial geometric points are then assigned a random value for the encryption process. Each facial geometric point is then assigned with random values to use as key for the homomorphic encryption process and the file is encrypted and stored in the NAS storage. The facial login prompt is also provided to the user for decryption of the file. Each individual user was assigned two unique random keys dynamically for encryption process based on the facial geometry. No keys were duplicated during the process, the storage is designed in such way to incorporate separate storage for users. The user interaction with the system is tested on 1000 unique logins on server and the accuracy is found to be 98%. This implementation of the system is based on the real time user interaction that exists in present times. This system can be easily adaptable to the mobile computing.

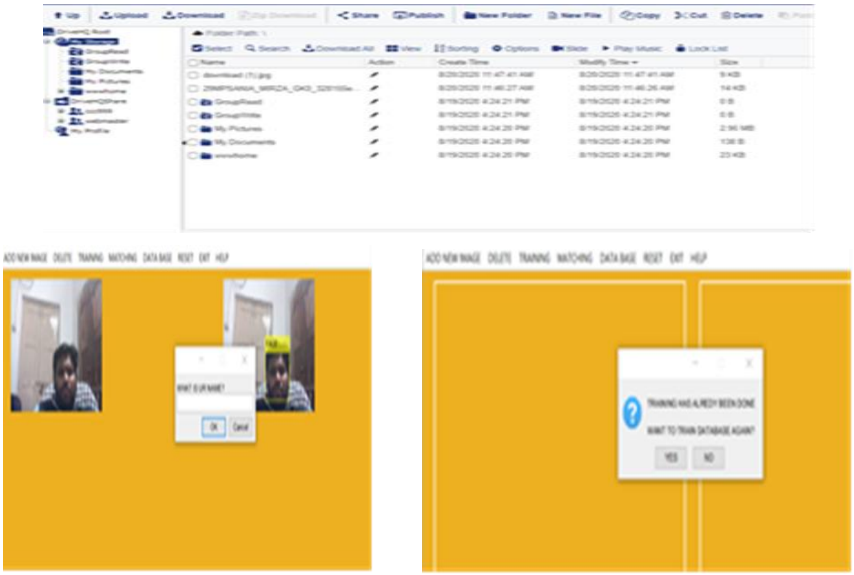

Figure: Facial Login portal with Training and Cloud Storage

Algorithm	Accuracy	Specificity	Sensitivity	Precision	Recall
PCA,WP&LDA	55%	50%	65%	55%	50%
GOBER WAVELET	65%	65%	68%	70%	62%
SVM	87%	81%	74%	78%	76%
Bayesian Classifier	88%	83%	80%	81%	79%
ANFIS	90%	85%	95%	86%	95%
CNN VGG16	97%	95%	78%	93%	96%
CNN VGG19	98%	96%	75%	96%	97%

Table: Comparing Parameters of Various Algorithms

CONCLUSION

The above procedure successfully implemented the cloud computing security using facial homomorphic encryption. The procedure was initially planned to be implemented on the fuzzy neuro system but the accuracy is found to be less on the procedure. In spite of continuing on the same trajectory the algorithm is updated to CNN where the system is first designed to recognize deep facial features. The based on the deep facial features the facial geometric points were extracted from each individual face. Then the facial recognition based on the facial geometric points were designed and implemented the accuracy in this process was more efficient than fuzzy neuro system. So the procedure is applied to the real world problem of the cloud storage. Since the mobile computing is on the raise and various privacy concerns were raised during present times the current procedure is assigned to the problem. This procedure successfully tackles the problem of the cloud security by implantation of the facial homomorphic encryption based on facial geometric points that were assigned during the CNN deep facial features. Each unique key is designed based on the facial geometric points the key generation is based on 8-bit random facial keys that are obtained by the algorithm. The web based login is also developed on the basis of the flask framework that implements the CNN (VGG 16 network) procedure and the app hosted on the Heroku server and a NAS storage is attached to the server. This constitutes end to end cloud storage with deep facial features using a homomorphic encryption. The user testing was done on various devices to store files of various kind user of various ages are also tested for the login portal. The login creates the facial geometric points and creates a node for each individual user in the network. The node is also having a unique random key for encryption and decryption. This process is successfully tested and the accuracy is found to be 98%. This methodology successfully implemented cloud storage on server and tested on various devices. This attempt to solve privacy issues was successfully tackled by the current system and can be applied to real world problems.

REFERENCES

- *Nitin Chauhan; Laxmi Ahuja; Sunil Kumar Khatri2018 International Conference."Secure Data in Cloud Computing Using Face Detection and Fingerprint".*
- *2018 IEEE Symposium "Cloud-Vision: Real-time face recognition using a mobile-cloudlet-cloud acceleration architecture"Tolga Soyata; Rajani Muraleedharan; Colin Funai; Minseok Kwon; Wendi Heinzelman*
- *"Cloud Based Big Data Analytics Framework for Face Recognition in Social Networks Using MachineLearning"2015Procedia Computer ScienceA.VinayaVinay S.Shekhara J.Rituparnab TusharAggrawalb K.N. Balasubramanya Murthya S.Natarajanb*
- *"Cloud-Vision: Real-time face recognition using a mobile-cloudlet-cloud acceleration architecture" 2012 8 IEEE SymposiumTolga Soyata; Rajani Muraleedharan; Colin Funai; Minseok Kwon; Wendi Heinzelman*
- *Li, C., Wei, W., Li, J. et al. A cloud-based monitoring system via face recognition using Gabor and CS-LBP features. J Supercomput73, 1532–1546 (2017). https://doi.org/10.1007/s11227-016-1840-6*
- *"Privacy Preserving Face Identification in the Cloud through Sparse Representation" Xin Jin Yan Liu, Xiaodong Li, Geng Zhao, Yingya Chen, Kui Guo October 2015*
- *"Privacy preserving security using biometrics in cloud computing" Authors: Santosh Kumar,Sanjay Kumar Singh,Amit Kumar Singh, Shrikant Tiwari, Ravi Shankar Singh Multimedia Tools and Applications Volume 77Issue 9May 2018.*

- *"Cloud-Based Face and Speech Recognition for Access Control Applications"Nathalie Tkauc; Thao Tran; Kevin Hernandez-Diaz; Fernando Alonso-FernandezIEEE Conference on Communications and Network Security (CNS)*
- *"Multiple face recognition in real-time using cloud computing, Emgu CV and Windows Azure"Diego von Söhsten; Sérgio MuriloInternational Conference on Intelligent Systems Design and Applications (ISDA)*
- *Zhou, S., Xiao, S. 3D face recognition: a survey. Hum. Cent. Comput. Inf. Sci.8, 35 (2018). https://doi.org/10.1186/s13673-018-0157-2*
- *Wang, W., Lin, H. & Wang, J. CNN based lane detection with instance segmentation in edge-cloud computing. J Cloud Comp9, 27 (2020). https://doi.org/10.1186/s13677-020-00172-z*
- *Liu, J., Wu, J., Sun, L. et al. Image data model optimization method based on cloud computing. J Cloud Comp9, 31 (2020). https://doi.org/10.1186/s13677-020-00178-7*
- *Yin, Y., Lin, J., Sun, N. et al. Method for detection of unsafe actions in power field based on edge computing architecture. J Cloud Comp10, 17 (2021). https://doi.org/10.1186/s13677-021-00234-w*
- *Padilla, R.S., Milton, S.K. & Johnson, L.W. Components of service value in business-to-business Cloud Computing. J Cloud Comp4, 15 (2015). https://doi.org/10.1186/s13677-015-0040-x*
- Padilla, R.S., Milton, S.K. & Johnson, L.W. Components of service value in business-to-business Cloud Computing. *J Cloud Comp*4, 15 (2015). https://doi.org/10.1186/s13677-015-0040-x
- Xu, Z., Zhang, Y., Li, H. *et al.* Dynamic resource provisioning for cyber-physical systems in cloud-fog-edge computing. *J Cloud Comp*9, 32 (2020). https://doi.org/10.1186/s13677-020-00181-y