International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Neural Network Optimization-Based Facial Geometric Key Homomorphic Cloud Security

Tadi. Chandrasekhar[1], Ch. Sumanth Kumar[2]

Submitted: 28/10/2022 **Revised:** 18/12/2022 **Accepted**: 04/01/2023

Abstract: In the modern day, cloud computing has become an essential component of technological and individual interactions with computing devices. The majority of cloud platforms use conventional encryption techniques for device authentication, whereas the cloud services that are still useful offer consumers older protocol for device authentication. The face authentication protocol described in this work will provide a facial geometric point that will serve as the encryption key. The method was created as a multi-stage implementation of the interdependent facial recognition algorithms. The fuzzy neural inference algorithm, which forms the basis of the first sequence of the algorithm, is used to implement face verification of users and the input of each person into a tracking sheet. The second method involved facial geometric point mapping of a face for the recognition of deep facial features using a convolution neural network (CNN) using a VGG19-based architecture. A facial geometric point-based facial network was created based on the algorithm, and each unique face was given a label. The process added the ability to recognize numerous faces in a single image. The third approach makes use of a cloud authentication system that is based on face geometric point identification. Based on facial geometry points that will be used as input for the encryption cypher, this method generates a dynamic encryption key. In order to encrypt the file, these facial geometric points, which are calculated based on the number of regions that were detected on a particular face, are given a dynamically assigned value and input to the key of the specific algorithm. These geometric points will also be used to decrypt the file.

Keywords*: Encryption, Facial Features, Algorithm, Recognition*

1. Introduction

Constant facial recognition is included into biometrics. The term "biometrics" refers to a computer's capacity to identify a person based on an exceptional actual trademark. The limit of a PC's ability to recognize a person based on their facial features is face recognition. One of the areas of trend-setting innovation that is expanding the fastest is biometrics. According to predictions, biometrics will become widely used in the twenty-first century to verify identities [10] and prevent unauthorized access to institutions, databases, and workplaces. A facial recognition tool compares an image or video of a human face to other pictures of faces stored in a database. The construction, shape, and extents of the appearances are taken into consideration throughout the face ID processes. The distances between the eyes, nose[8], mouth, and jaw, as well as the top forms of the eye attachments, the sides of the mouth, the positioning of the nose and eyes, and the region enclosing the actual eye bones, are also taken into consideration. Using a face recognition tool, a few images of the individual should be taken at various angles and with different expressions. The individual briefly faces the camera while providing affirmation and distinguishable proof, and then the image is put up against those that have recently been taken [9]. Facial recognition is frequently utilized due to its advantages. The benefits of facial recognition include the fact that it is non-intrusive and may be done from a distance without the subject being aware that they are being filtered. Face recognition systems are superior to other biometric methods in that they can be used for observation purposes such as the search for necessary lawbreakers, suspected fear-based oppressors, or missing children. Since it is easy to change someone's face and a cover can be used to conceal the person, face recognition developments are more useful for facial verification than for distinguishing proof [11]. The weather should be taken into account, along with topic developments and camera centre. When combined with another biometric technology, facial recognition could significantly enhance verification and appreciable proof results. Face recognition has caught the attention of researchers in the fields of safety, brain science, and image processing. It takes into account a sizable report field. An important application of facial recognition is to support legal requirements. In order to quickly reduce the number of suspects, officials may benefit from the scheduled recovery of suspect images from the police mug-shot information base. Face recognition software calls for a

[1]*ECE Department, ISTS Women's Engineering College, Rajahmundry, India*
Email: ramyoga.2011@gmail.com, ORCID ID : 0000-0002-1945-2977
[2]*ECE Department, GITAM University, Visakhapatnam, India*
Email: sumanth336@gmail.com. ORCID ID : 0000-0001-7410-4943

constant response, and running it on a mobile device makes it portable because it is accessible from anywhere. The attempted solutions always increase complexity and execution durations, yet they are incredibly difficult to implement in terms of a cell phone's energy [12], processing capability, and information storage. Flexible distributed computing addresses the cell phone asset issues that fundamentally impede the enhancement of administration quality by shifting computing power and data storing away from mobile devices and into the cloud. It makes applications and portable figuring accessible to a much wider range of portable supporters, providing these features to both cell phone users and the wider range of portable supporters. Customers will genuinely desire to access a variety of new components that will update their phones because of Mobile Cloud Computing [13]. The security of mobile devices has been improved through intensive cloud-based programming observation and maintenance.

In this paper, we examine face-recognition methods. We divided the methods into three categories: feature-based, holistic, and hybrid approaches.

This paper's main contribution is to:

- Identify various facial recognition techniques;
- Recognize deep facial features using neural networks
- Assess deep facial homomorphic encryption.

2.Connected Work

Because of the considerable development of AI, the PC environment, and acknowledgment frameworks, numerous analysts have made inroads towards design acknowledgment and recognized proof using various biometrics using various emerging mining model philosophies. [1] suggested an innovative strategy for dealing with the problem of programming emotion recognition across many modalities. [3] offered a novel approach to the problem of moving toward programming emotion recognition across many modalities. The researchers suggested a novel approach to the problem of figuring out how to programme feeling acknowledgment across many mediums. The provided model for look recognizable proof to communicate information from a self-assertive [4] proposed a novel approach to move finding out how to programme feeling acknowledgment across various saliency maps. The suggested method is free of the model as experience is only shared through the expansion of information. The evaluation revealed that the new model had the ability to adapt to the new area more quickly when the proposed model was forced to focus on the information bits that were regarded significant sources. In light of an exchange learning technique and a Convolution Neural Network, [2] developed a programmed facial acknowledgment framework. CNN makes use of the loads obtained from the created VGG-16 model. The Archive Face [3] suggested additional substance precise edge loss to achieve face recognition. The suggested Archive Face has unquestionable mathematical knowledge because of its precise link to geodesic division on a hyper sphere. Additionally, they presented the most in-depth exploratory evaluation of the FR technique using ten Face Recognition datasets. They claimed that Archive Face consistently defeats the competition and may be used with no processing expense. The confirmation execution of open-source Face Recognition models was 99.82 percent on the Labeled Face Wavelets dataset, 95.45 percent on the Center Abled Face Wavelets dataset, and 92.08 percent on the Counter Point Labeled Face dataset, respectively. To create organized data sizes for face affirmation systems, space express data advancement was introduced. By dealing with the countenances in the datasets and using standard convolution neural nets to order request photographs, they demonstrated how to handle on practical datasets with important facial variants. They rigorously tested their framework by subjecting it to the labeled Faces benchmarks and Janus on numerous downloaded images. They declared the customary display for unfettered, segregated external data and stated that the average accuracy of their data collection was 100% error rate. [7] created a crucial framework for administration before cutting-edge secret sharing. This work's goal is to provide a more dependable decentralised lightweight key administration method for cloud frameworks that will advance key management and information security [14]. The suggested arrangement ensures the confidentiality and protection of customer data by replicating critical offerings over many hazes while using a mystery sharing instrument and a democratic strategy to guarantee share respectability. The technique used in this concentration also improves defense against byzantine failure, server intrigue, and information manipulation attacks.

3.Methodology

The methodology adheres to the different procedural components. The YALE and ORL dataset is the dataset that was utilized in the early implementation of the face security of the users using fuzzy neuro inference networks. The same dataset's facial geometric points were employed in the second procedure to extract the deep facial characteristics, and CNN (Convolution Neural Networks) with the VGG19 network was the algorithm used. The Deep Face Feature Training of the VGG16 network and a custom network with 100k samples were utilized to process the facial geometric points for celebrity facial recognition. Deep labeling techniques were used to produce multiple facial feature

recognition for celebrities. During the authentication and encryption step, the last phase implemented the face geometric points for cloud computing security. This phase built a camera-based login portal for a facial cloud weblog. The facial sample collection will serve as the training phase of the authentication system, and the cloud login site will serve as the testing phase. After that, random facial points collected from the phase were utilized to encrypt the files using facial geometric points.

3.1 Automated Facial Recognition Using Fuzzy Neuro Inference Networks:

A fuzzy neural network is a FNN (U, W, X, Y, L) structure that meets the requirements listed below:

a. U is a sample container for the Fuzzy Neurons' facial template.
b. The weight matrix W corresponding to the image parameters of the fuzzy neural network is determined by the matrix product $U \times U \rightarrow DW$ (DW weights of the facial features).
c. The input image maps are what the image vector inputs XDX refers to (DX is domain of input maps)
d. The output image mappings are described by the image vector outputs YDY (DY is the domain of the output vector).
e. The input and output maps' images will be used to train the learning algorithm L.

Figure: ORL dataset images

Figure: Yale-B dataset images

While some fuzzy neural networks lack some of the essential structural traits of neurons, others are based on fuzzy logic processes. The input neurons are initially provided the training photos, and each image with its accompanying facial traits is processed as a node in the training network. The facial feature neuron and its derivatives are fundamentally stored as processing units. Each image is examined based on the face neurons that were trained to the network using the facial feature units that are kept in the form of a fuzzy network.

3.2Using CNN, Facial Geometric Points

The three-phase arrangement of the Convolution neural network structure serves as the foundation for the facial geometric points.

a. Face Recognition
b. Identification Mode
c. Tracking of faces

a.

Face Recognition

A fundamental component of facial geometric point detection is face detection. The Convolution Neural Networks' division of the micro resolution serves as the foundation for the facial detection calculation. Convolutions layers (used only in 3*3 size), Max pooling layers (used only in 2*2 size), and Fully connected layers at the conclusion are used to create picture pyramids from each face sample that is processed through the procedure for the assemblage images. This allows for the detection and arrangement of faces. The group describes the image regardless of whether it is facial or not. The complete recognising face image is shrunk to 160x160 pixels prior to acknowledgment.

b.Identification Mode

Based on the network layers created by convolution neural networks, a neural network-based system for facial recognition is created. High-performance computing is being used here. The VGG16 serves as the foundation for this methodology. In order to accomplish this, we used a VGG16-assembled face acknowledgment strategy based on Inception engineering, in which we saved the layers of the identified countenances in a mat record and a h5 document for acknowledgment. The idea is to enlarge the essence of a different individual to be distant while decreasing the information picture's insertion into a similar individual's component area. Here, it is also suggested to use a facial key marker to identify a specific area of a face in a photograph based on the pose of the subject. In the location stage, we also create an xml document with the name of the connected face.

c. Tracking of Faces

The planning time is a crucial concern in the face recognition system for the current application since it depends on the cycles of each progression, such as face location, face plan, and face recognition itself. In our tests, face recognition took a long time to process for each case when we applied it to the whole image of every edge in the picture. When a face is seen, we anticipate that it will only be present for a brief period of time. To follow the face involving a relationship channel that was subject to estimation in this way, we used calculation. Then, in order to determine whether a face may be linked to a document name, the perceived face from the h5 and mat documents is contrasted with the xml data. The crucial indicators are then linked to a specific area of a face that possesses the characteristics.

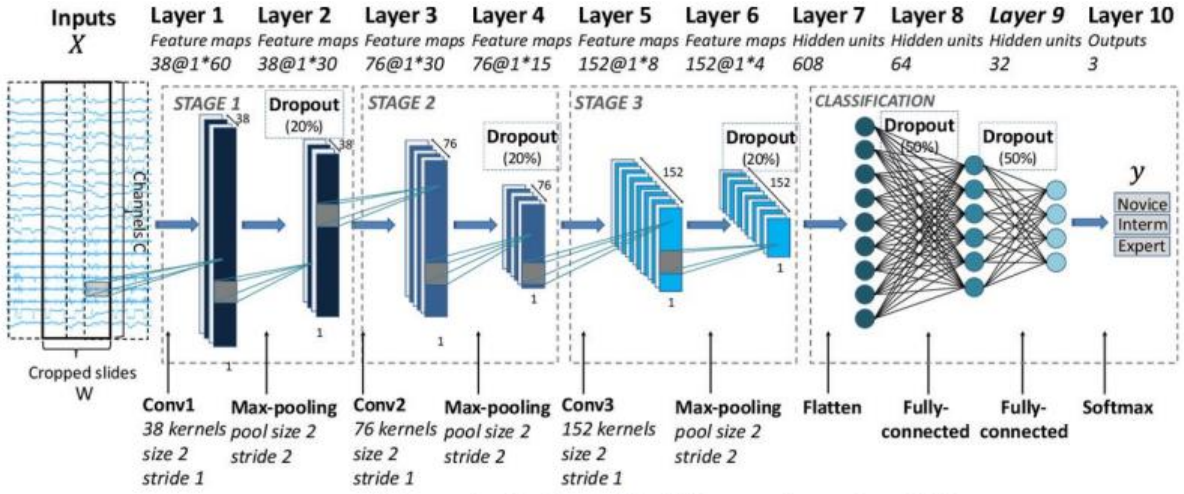

Figure: Applications of facial key markers using CNN

Every single one of these models cited the inability to plan data as a major obstacle to developing reliable models. Some then moved on to larger 3D item deceptive models or instructional recordings. We present a significantly simpler alternate option and demonstrate how it may result in consistent repetition of various task and application names in paper titles relating to two of the most significant key phrases.

4.Cloud authentication

There is also a cloud server in this design. A Network Attached Storage server, which may be sent on a variety of equipment stages and uses minimal resources, is required for this reflection. As a result, the file is split, and the homomorphic encryption method is used to send the request. The face test camera input serves as the first step in the approach and serves as the encryption key for the record. The record is then managed and removed from the cloud server's storage after that. The client's face input is used as a key in the file's decryption during the recovery approach.

Algorithms

4.1.Fuzzy Neuro System

Fuzzy logic is implemented by a fuzzy neural network in a variety of ways, including the information yield level, neurotransmitters, the conjunction cycle, and, surprisingly, the initiation work. To build a precise numerical representation of the fluffy neural organization, we'll use the language used in x is the fluffy information vector and y is the fluffy outcome vector, both of which are fluffy whole numbers or stretches. The association weight vector is denoted by W. We could numerically describe the accompanying planning from the n-layered info space to the l-layered space:

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

A conjunction activity does not completely determine how similar the association weight vector and the fluffy information vector x(n) are (n). Although the juncture activity characterizes a number juggling activity in fluffy neural organizations, such as fluffy expansion and fluffy augmentation, it shows a summation or item activity in neural organizations.

The following nonlinear operation is implemented by the output neurons:

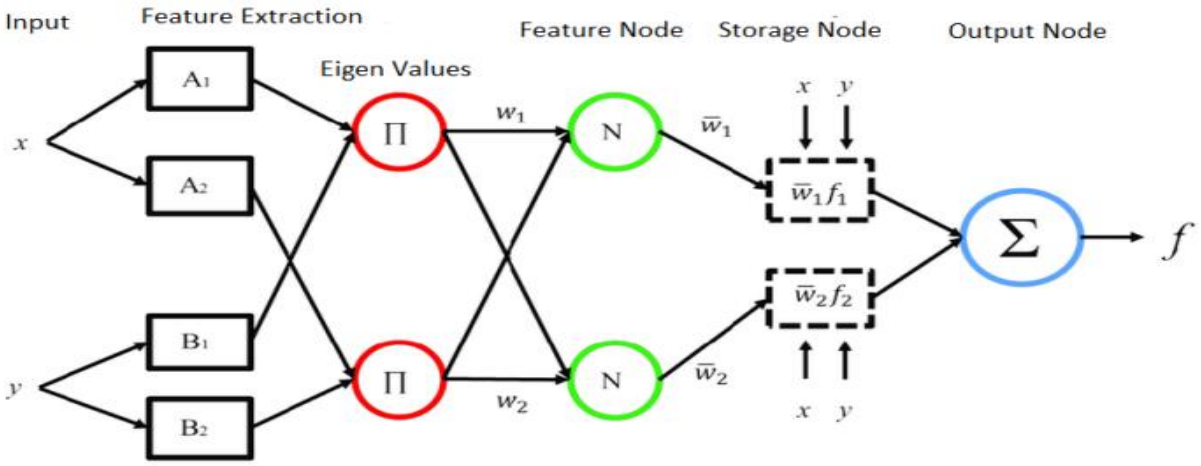

Figure: Fuzzy Neuro System Block Illustration

(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 a distance in Rl is defined by d(). The fuzzy neural network's learning algorithm, W(n+1)=W(n)+W(n), modifies the weights of the NW connections in the network.

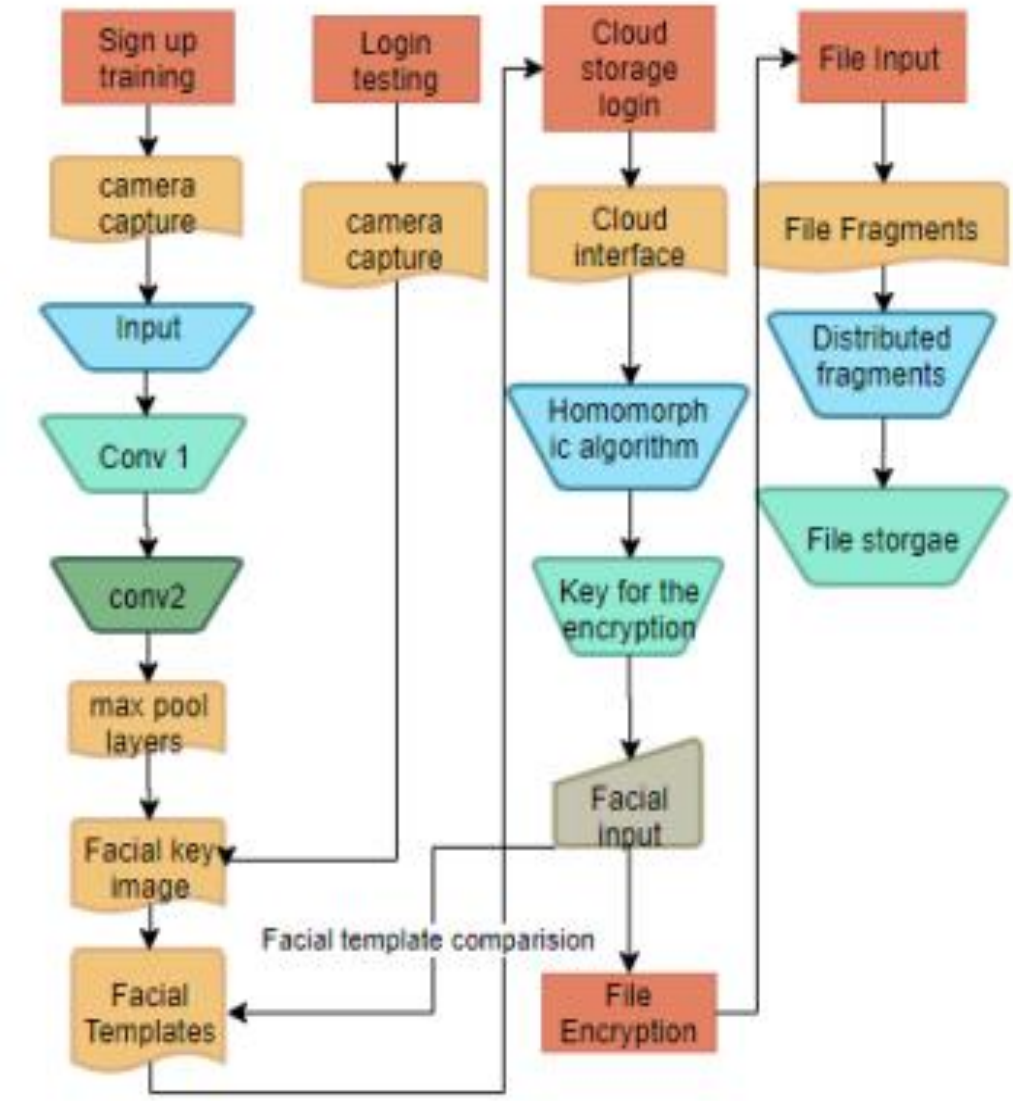

Figure:The Architecture of the facial key based cloud storage

4.2

Convolution Neural Networks

The subsequent neurons are interconnected and were being assigned weights

$w^{q}_{j,s}$, q= {-Q, …,0, …, Q} connected by the filter $€^{\mu}_{e,r}$. Users' inputs will be collected for Convolution Layer and its associated parameters, t, and s.

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

The sample collection phase denoted by €µe, k' cµ i, p.Each sample is collected and indexed with {e,k} p and k $h^{u}_{j,q}$.

$€^{\mu}_{j}$ setting r=q + t, the position is set to q and is the translation vector. The hidden layers' pixel array's hidden features are indicated by

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

Resolution for the maximum pooling layer changes when the sample's micro resolution parameter changes as $\Delta T^{d}_{j,k}$.

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

Where $\delta^{\mu} J_{j,q}$ is the picture with the more detail

$\delta^{\mu} J_{j,q} = \Sigma_t F \mid (g^{\mu} j, q)\ \Sigma_i \delta^{\mu}{}_{i,q-s} v^{s}{}_{i,j}.$

The following equation describes the RELU layer of the CNN with the indexing parameter and all of the patterns analyzed by the system.

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

The fully connected layer's input is the parameter k and is given by $\{\delta^{\mu} I_{j,q}, {}_{\Delta} I^{d} j, \delta^{\mu} I_{i,p}\} = \{\delta^{\mu} \mid j, q, \Delta I^{d}{}_{j}$ and $\delta^{\mu} I_{i,p}\}$, I is the picture that was transmitted to the output layer. The filter length of the output layer is specified as the indexing parameter values of s= -S..., 0..., S, and 2S+1. The output layer is described as

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

Features for the output layer's spatial feature weight shifting and the resulting cost function, which is defined as

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

The random keys created by the algorithm are of 8-bit

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

value and the values of m range from m=-m,0....,m. From the equation above, h and g are the algorithm's face features. Additionally, the following will be used to decode the FIE:

The server's files will be in a format that is randomly fragmented, with all of these fragments being linked together in multiples.

$F = 0.5\ \Sigma\mu_{,k,q}\ [D^{\mu}{}_{i,p} - M^{\mu}{}_{i,p}]^{2}$

The system's training component will be responsible for the entire process, and a network file that results from it is kept in the system's root directory. The equations specify the testing portion. Each image is subjected to four or five equations of processing before being compared to the network file and identified for their subsequent inclusion. If the image matches, equations four or five will constitute the key points. The face region displays six major points.

4.3.Homomorphic Encryption on the on cloud

The input file that had undergone homomorphic encryption f $\oplus$ kand f file with key k. [[f]]=Enc(f, k)=f $\oplus$ k. The encrypted file [[f]] is existing in the storage. The following criteria must be met in order for a cloud storage file to be decrypted: f=Dec([[f]],k)=[[f]] $\oplus$ k. And the key is defined by the following.

Results

The Fuzzy Neuro System is used to start the process of Facial Authentication in the cloud computing system. The facial neuron channeling of the face features, as previously stated, is implemented in this system. The approach collects facial templates from 100k samples using the YALE and ORL datasets. The facial camera samples of non-dataset individuals were gathered and the fuzzy neuron was trained using the dataset information. Along with the users from the dataset, 1000 users were employed in the training procedure. Fuzzy system is used to store neurons in the network of neurons based on the data. The accuracy was determined to be 92% on these samples, and several other characteristics are discussed below.

Figure: Fuzzy Neuro System Face Recognition

Based on the face geometric points that are based on the same dataset, the second component of the cloud security implementation is produced. The dataset's facial templates were utilised to develop the CNN algorithm with VGG19 networks for the recognition of deep features. The deep characteristics estimated by CNN are used to create the facial geometric points. The CNN algorithm has several layers that are used for processing, and the output layer of the algorithm is where the features are stored. By computing the facial geometry outlined above, the facial geometric points are presented on the face.

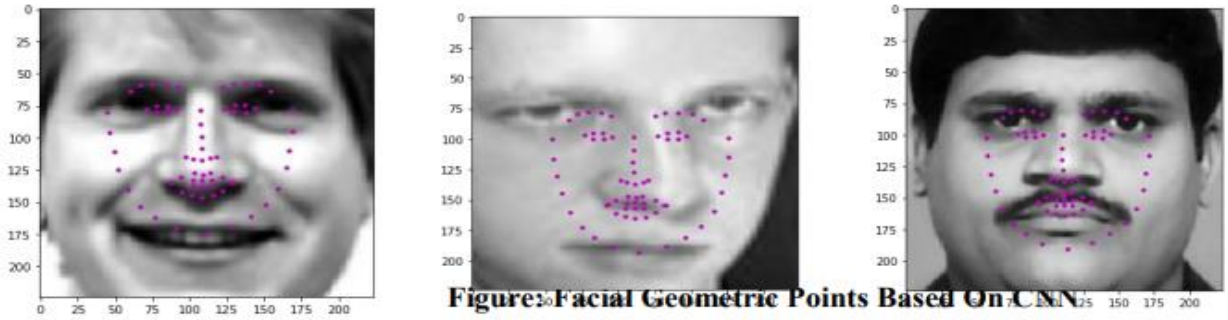

Figure: Facial Geometric Points Based On CNN

Then, using datasets from Korea's black, pink, and white population, the algorithm started to recognize many faces of famous people. 200 000 samples have been collected in accordance with the law. Each celebrity was taught on their unique face, and testing was done on group photos where each face had facial geometric points that had been assigned names based on the facial geometry. This face geometric point approach is further applied to user security in cloud computing.

.

Figure: Multiple Facial Recognition Based on Facial Geometric points

The cloud portal's web-based login, which was created using the Flask framework and hosted on the Heroku server, uses live captured photos as input to calculate the facial shape. The private cloud server was created using NAS technology storage. Based on the developed algorithm, each user signup procedure was prompted with live user sample collecting from the web camera, the user's information was kept in the CNN network log file and database records. This procedure is the training procedure. Based on the geometric points that the programme retrieves, the facial geometry is determined. The random value for the encryption procedure is then assigned to these face geometric points. The file is then encrypted and stored in the NAS storage. Next, random values are assigned to each facial geometric point to be used as the key for the homomorphic encryption procedure. The user is also given the option to decrypt the file using a face login prompt. Based on the geometry of the face, two separate random keys were dynamically assigned to each individual user for encryption. Since the storage is set up to include user-specific storage, no keys were duplicated during the operation. 1000 distinct logins to the server are used to test how the user interacts with the system, and the accuracy is found to be 98%. The real-time user engagement that exists in the present is the foundation for this system's implementation. This system is easily transportable computing adaptable.

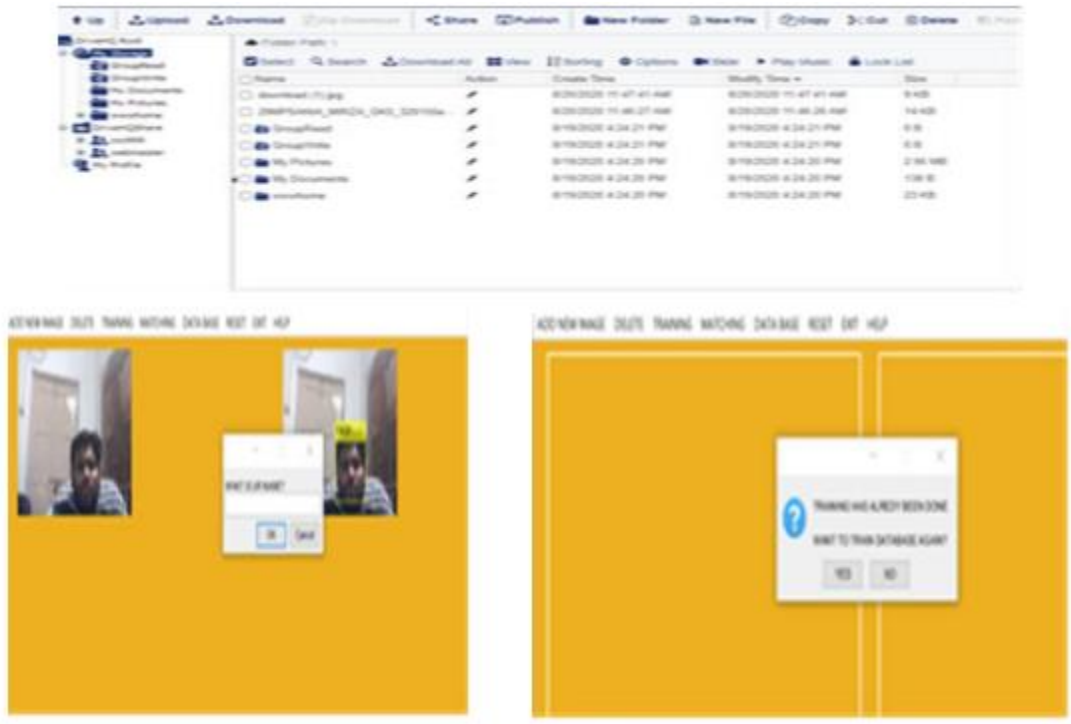

Figure: Facial Login portal with Training and Cloud Storage

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

5.Conclusion

The aforementioned process was a success in implementing facial homomorphic encryption for cloud computing security. Originally intended to be used with the fuzzy neuro system, the approach has been shown to have lower accuracy. The algorithm is updated to CNN, where the method was first developed to recognise deep face features, albeit continuing on the same path. The facial geometric points from each unique face were extracted based on the deep facial traits. Then, a facial recognition system based on geometric points on the face was developed, and its accuracy outperformed fuzzy neural systems. The solution is therefore applied to the cloud storage problem in the real world. The problem is assigned to the current technique since mobile computing is growing and numerous privacy concerns have been raised recently. By implementing face homomorphic encryption based on facial geometric points assigned during the CNN deep facial features, this approach effectively addresses the issue of cloud security. The key generation is based on 8-bit random face keys that are obtained by the algorithm, and each unique key is designed based on the facial geometric points. The programme is hosted on a Heroku server, and a NAS storage is connected to the server. The web-based login is also constructed using the flask framework, which implements the CNN (VGG 16 network) technique. End-to-end cloud storage using homomorphic encryption and

detailed face features is what this represents. Users of different ages were tested for the login portal while using different devices to store files of different types. The login process creates a node for each unique user in the network as well as the face geometric points. The node also has a special random key that can be used for encryption and decryption. This procedure has undergone successful testing, and the accuracy is 98%. This methodology tested on multiple devices and successfully established cloud storage on a server.The existing method successfully addressed this attempt to resolve privacy issues and can be used to address issues in the actual world.

References

[1] Nitin Chauhan; Laxmi Ahuja; Sunil Kumar Khatri2018 International Conference."Secure Data in Cloud Computing Using Face Detection and Fingerprint".

[2] 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

[3] "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

[4] "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

[5] 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

[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

[7] "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.

[8] "Cloud-Based Face and Speech Recognition for Access Control Applications"Nathalie Tkauc; Thao Tran; Kevin HernandezDiaz; Fernando Alonso-FernandezIEEE Conference on Communications and Network Security (CNS)

[9] "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)

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] Xu, Z., Zhang, Y., Li, H. et al. Dynamic resource provisioning for cyber-physical systems in cloud-fog-edge computing. J Cloud Comp9, 32 (2020). https://doi.org/10.1186/s13677-020-00181-y