A Noval Method for Cloud Security and Privacy Using Homomorphic Encryption Based on Facial Key Templates

Tadi Chandrasekhar
ECE Department, ISTS Women's Engineering College, Rajahmundry, India
Email: ramyoga.2011@gmail.com

Sumanth Kumar
ECE Department, GITAM University, Visakhapatnam, India
Email: sumanth336@gmail.com

***Abstract*—In the technology era, data is the key aspect, and securing the data is also an important task as many of the utilizers' presence online is on an incremental trend. There is a sustainable requirement to indulge the security procedures to secure the vulnerable data within cloud computing. In this regard, facial recognition is the latest technological trend in the field of biometrics and it is regarded as a fast processing technique that is available in computing devices as well as on mobile devices. The cloud computing services that include Microsoft, Google, and Amazon are utilizing different types of encryption techniques to include the aspect of privacy. The present method deploys a methodology that furnishes facial authentication and the generation of facial keys for the protection of data. The cloud mechanism is processed by facial features for authorization and authentication. The facial templates database is furnished for cloud encryption of each file that is integrated into the core algorithm of the method and the facial key is compared with the templates of the face data and later it is encrypted. The observed outcome of the study furnished a methodology that can guarantee that the information of the cloud user and the reclusive identification of the person is secured. In this study, the creation of a double abstraction methodology is performed to assure data protection on a cloud computing platform by utilizing facial templates as an important aspect of the process of encryption. The outcomes of the study show superior aspects to the state-of-art techniques.**

***Index Terms*—facial recognition, bio-metrics, securing, cloud mechanism, facial template, key features & CNN**

I. Introduction

The technique of facial recognition is an eminent field with a scope of an extensive range of research like computer vision and graphic process that can be utilized in various systems and the techniques, include attendance and security systems like camera-based surveillance, recognition of identity, recognition of emotions, the technology is also extended in the field of robotics to identify any object. Detection of the face is the basic step taken towards recognition of the face. The human facial recognition process and the sampling process continue with the collection of different samples of the subject and their faces. Different retrieval angles of the face characteristics are analyzed and tested with different facial characteristics. Recognition of individual faces is not a challenging task, but when it is pitted with lots of faces that are stored on the security server of an organization, then the time that is utilized to remember each face is more. Even though this is the case, recognition of faces for the process of computation will be a contender for security systems which makes the cloud mechanism get a safe and authenticated methodology that can be utilized during the storage process. The mechanism that provides access drives the organizational structure. Important studies have utilized cloud computing for solving storage and authentication problems. Cloud computing technology is an on-demand service that, often in cases, is not operated on local computing storage in which the entire system is wired into an interconnected network of data centers that utilizes the particular protocols to be connected. In the frame that seeks to furnish scalability [1] via utilizing this approach, computing is performed whilst including huge data volumes stored within the data center. Because the process of computing is not processed within a local computer, the utilization of web-service communication which connects the clients with the server of the cloud, this methodology is performed often through various platforms which utilize SOAP or REST-API and other authorization protocols. Because cloud computing is generally inclusive of mobile computing as well as IoT devices as it contains limited resources for computing to process information [2]. The process of third-party computing mitigates the programming limitation which connects to resources that have the utilization of different connecting patterns and such a process can overcome the aspect of web services which would be interconnected to the response that is received from the interoperable mediums of exchange like JSON or XML files. The facial

Manuscript received April 26, 2022; revised July 6, 2022; accepted July 20, 2022.

doi: 10.12720/jait.13.6.638-644

recognition process includes various stages which require to be done mandatorily that starting with identification of the face, feature extraction, etc., Befitting and approachable hardware are required all the time as and when the facial recognition is being carried out and this process utilizes a substantial amount of time to process the data and the other inter relatable threads [2]. There are different confinements to the face identification system to perform the process of interaction with the cloud platform. The present study is an attempt to implement the CNN for facial key algorithm for the recognition of face as a fundamental to access cloud computing. The system can do facial recognition with limited resources and strong strategies for image processing and one such methodology is cloud computing research which is related to facial biometrics and is performed by 'face.com', that is an online facial recognition platform, which utilizes 'Facebook' as a provider of identity that utilizes graphical API [3]. The facial bio-metrics are performed in the robotics field to recognize human subjects and are performed by the utilization of local interconnected networks [4]. Further, the investigation is performed by creating an actual time depending on the log entry methodology. The past studies were performed depending on the local storage methodology which will authenticate the complete process and maintains the sampling. This methodology is changed and the dual server mechanism has been taken into consideration, to maintain the load within the storage as well as the process of authentication. The requirement for authenticating the server as well as the storage server is required to maintain the layer separation to implement. Further, confidentiality and privacy are the two major aspects of cloud platforms [5]. However, this study is based on trials that are conducted on different subjects. With the utilization of the extreme learning method and the study is proposed to perform face identification on large sets of facial databases. Further, facial recognition is an authentic methodology in the field of cloud computing for the data protection enhancement that is shared via dimensions that can be found in an open cloud [6].

II. Literature Review

The cloud computing systems furnishes easier access to the resources as well as computational data which are distributed over different cloud platforms [1]. The existing literature that is available for the technique of facial recognition is reviewed below.

The first step in this regard is storage operation within the cloud platform by the utilizers for the process of execution of different queries which would be given as input to the system running time [4]. On par with the results which are acquired by considering the various queries which are given by the consumer side, the architecture utilizes the layers of the security mechanism by maintaining the concealment of the vulnerable information for the provision of security aspects to the utilizer [7]. The facial samples which are collected for the biometric data of different users can be secured and stored within the cloud server. The data which is stored and secured is termed to be authentic data and the information confidentiality from the processed samples of data is not encrypted [8]. Henceforth, the utilizer of the base cloud should be authorized and given access to the resources within the cloud platform by the utilization of their biometric-based identification system which will authorize via storing the biometric data [9] and it has different advantages as well as it creates typical sorts of vulnerabilities. The furnished vulnerabilities include the control of access and in certain cases; it creates leakage of information, loss of data as well as security breaches. A typical study into the procedure of authorized cloud systems which enterprises can seek to have complete privilege access to save and process the data by giving access to the original information to store the biometric data [10]. The data storage and the techniques utilized are found to be ineffective to process the data which is in the cloud server. Biometric data which includes securing privacy is proposed by maintaining the confidentiality and the completeness of the biometric information which is stored is to be given access by a public key which is encryption based one [11]. The past mentioned technique works faster and in this, the servers are unable to work and inappropriate to identify from the stored and secured biometric data of the clients and their respective enquirers which are processed to the server. The utilizers who are present in the server of the cloud are not capable to get the different contents of the face sample without the conventional approach determination as token depended on identification and password-based identification. The algorithms which are furnished can only be applied to the trusted servers [12]. The present study focuses on the assumptions which are derived from the standard protocols which are algorithm based. In other cases, the biometric samples which are secured and stored in a facial database are not given complete access and this resulted in the utilization of different techniques like encryption to store the data within the database [9], [13]. The latter studies depend on the algorithm which deals with important issues like data leakage which is stored in the cloud using bio-metrically and security worm holes etc. Here certain sorts of major privacy securing problems are included by the researcher, and the induced biometric authorization framework to ensure the data privacy of the utilizer's that is present in the cloud platform. Similarly, the framework which advances the protection of privacy of the utilizers of the cloud by utilizing biometric properties is introduced by the researchers. The identification of different facial images depends on the eigenfaces algorithm which is utilized in the proposed system [14]. The system of authentication and authorization which authorizes the cloud utilizers is a cryptosystem public key encryption scheme [15]. The methods of the encryption will complete the encoding of the biometric face properties of the individual and in this system; the encryption technique consolidates the process of encryption of the biometric data. The Euclidean distance method calculates the similarity matching values (scores) between query (test) face template that is stored within the face template database. The similarity matching algorithm executes on the computational basis of the scores of similarity which lies between the facial image query and the facial template database. The past systems contain enhanced efficacy by utilizing methods of encryption for authorization and encryption of the generated templates. The equivalent method by Huang *et al.*, [9], [16] proposes the procedure which is based on the authorized methodology by including the past techniques and they proposed that an enhanced paradigm for the computational purposes of the cloud-based biometric systems by separating the logic implementation and storage layers which extracts the properties of the patterns of the iris of the cloud utilizer's. This methodology utilizes authorization which performs the identification and verification of the person's eye pattern for the preservation of privacy by storing the templates of the iris within the server of the cloud [17]. In a study, the researchers have acquired an algorithm that utilizes a mathematical model to secure the data of the user. The major challenge which is encountered in this aspect is the protection of the privacy of the utilizers. Many studies are being performed to mitigate this aspect using retrieving the information and is related to metadata by utilization of the hashing functions. The basic advantage of the hashing function is that it mitigates the superfluity of the information which is securely stored in the wide range and database by exploring some of the characteristics of the data that is stored.

III. Proposed Methodology

A. *Facial Identification Based Homomorphic Encryption on Cloud Platform*

The prominent cloud computing systems which are available are as follows:

- Amazon Web Services (AWS)
- Google Cloud Platform
- Azure etc.

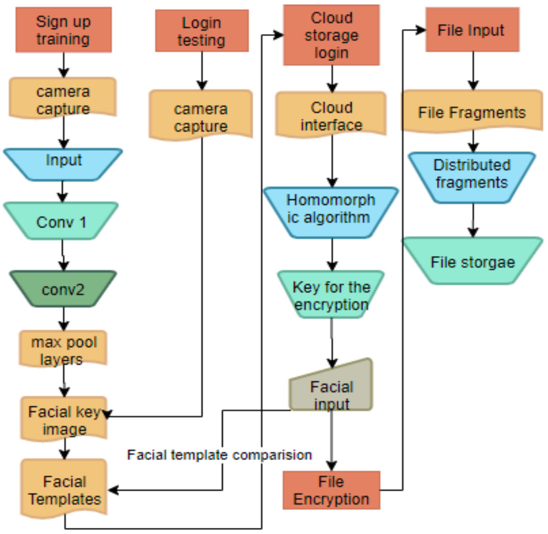


Figure 1. Architecture of facial key-based storage in the cloud.

Basically, within every cloud architecture, the utilizer has to negotiate with various protocols of security to acquire access to the cloud platforms. The present study aims at facial identification-based homomorphic encryption which is classified into various layers of execution. The Architecture of the Facial key based storage is shown in above Fig. 1.

- The first layer is the abstraction layer of the facial Identification that is implemented on an Authorized Server
- The second one is also an abstraction layer that depends on the cloud storage and in this encryption of individual files takes place.

B. *Authorization Server*

The authorization server is a machine within the cloud that recognizes and processes the faces and this server is separated from the storage server of the cloud. It contains samples of the faces which are collected from the utilizer and the samples that are collected are allocated to the memory for the process of retrieving. The machine which is allotted with this process is very resourceful since it has the capability of resolving the image processing maneuvers which are raised by the utilizers. The image processing layer is another layer that is attached to the server of the cloud and it can implement the process of authentication. The process of authentication is performed by identifying and capturing images of the utilizer and the utilizer faces are converted into the face templates and are analyzed for their key point by utilizing the Convolution Neural Network (CNN) architecture. The samples which are analyzed are then securely stored within the authorization server and the captured templates of the face are reused for the process of encryption and are furnished below.

C. *Cloud Server Integrated with Homomorphic Encryption*

The server of the cloud is another abstraction layer that is executed in this system. This is built on Network Attached Storage (NAS) server and it utilizes fewer resources when compared with other servers it can be utilized in multiple platforms of hardware. The storage process is undergoing via the input from the cloud utilizer and later the file is fragmented for processing and later the request is redirected to the homomorphic encryption algorithm. In this system, the process is prompted with the input of the camera for the face sample that acts as fundamental for the file encryption. The file is processed to the cloud server for storage purposes. The subsequent process is performed during file retrieving in which the utilizer is prompted with face input as fundamental file description.

IV. Experimentation

A. *CNN*

This is the first step in the authorization server in which the processing of the samples of the face is done by utilizing the cloud architecture. Every individual face is processed by capturing phase and is designated as $€^{\mu}{}_{k,r}, c^{\mu}{}_{i,p}$.

$\{i,k\}$= array indexes; p,k = neuron indexes and are designated by $h^{u}_{j,q}$

These neurons are interconnected to the preceding layer and the weights are distributed as a transitional network and they are designated as *wtj,k, t*= {-T, …, 0, …, T} and the filter which connects the input array is €μk,r and are directed to feature vectors *Vμj,q*. 2T+1 is the point of transition size of the region the weight of the network exists. The convolution layer μ hidden with its parameters j, q get the n inputs from the user.

$$h^{\mu}_{x,\,q}=\sum j\ \sum t\ \ w^{t}_{i,j}\text{€}^{\mu}_{j,\,q\,+t}+b_{x} \qquad (1)$$

€ μ j is termed to be a local position that is located on an image vector and the center of translation is q by setting $r{=}q{+}t$. The term bx is usually constant bias. The concealed properties are formed by the neurons of the array of the pixel and are derived by:

$$V^{u}_{j,q}=g(h^{u}_{j,\,q}) \qquad (2)$$

The neuron rotation is defined by the i^{th} pixel point array that is fed into the preceding layer and is given by:

$$h^{u}_{i\,,p}=\sum j\ \sum s\ \ w^{s}_{i,\,j}\,V^{\mu}_{j\,,\,p\,+s}+b_{i} \qquad (3)$$

The values of s={-S, ..., 0, …, S}, and 2S+1 are furnished as the length of the filter of the output layer, the index parameter is substituted by $q{=}p{+}s$ that does the absolute indexing that results in the final output layer designated by the final output of the network and is given by:

$$O^{\mu}_{i,\,p}=g(h^{\mu}_{i\,,p})=g(\sum j\ \sum s\ \ w^{s}_{i,\,j}\,V^{\mu}_{j,\,p\,+s}+b_{i}) \quad (4)$$

The positioning of 'n' no. Of filters within a sequence of order by hidden layers and this method results in large portions of the input vector with function.

$$O_{f}=f(\text{€}_{\text{p-}X\text{-}T},\ \ldots.,\ \text{€}_{\text{p}},\ \ldots,\ \text{€}_{\text{p+}\,X+T})$$

The maps with spatial features should be indexed with the utmost care because the weights are shifted from one to another in which the head angle is tilted in this case and it may lead to the weight adjustment and is described as:

$$E=\frac{1}{2}\sum_{\mu,i,p}\ [\mathrm{C}^{\mu}_{\mathrm{i,\,p}}-\mathrm{O}^{\mu}_{\mathrm{i,\,p}}]^{2} \qquad (5)$$

i = array index; p=corresponding image weight of the input image.

The derivative error of the g^{th} weight of the r^{th} filter of the t^{th} feature is described as:

$$\left.\delta E\middle/\delta W^{\,g}_{\,t,r}\right.=\sum_{\mu,r}\ [C^{\mu}_{i,\,r}-g(h^{\mu}_{i,\,r})]\,g^{|}\,(h^{\mu}_{i,\,r})\ V^{\mu}_{j,r+g} \qquad (6)$$

It is the combination with the natural gradient filter of weight and the update rule results in:

$$\Delta\ w^{s}_{i,\,j\,=\,\acute{\eta}}\sum_{\mu\,,p}\ \ \delta^{\mu}_{i,\,p}\,V^{\mu}_{j,\,p\,+s} \qquad (7)$$

CNN for image processing purposes, to store a processed image, is defined as follows:

$$\delta^{\mu}I_{\,i,\,p}=[c^{\mu}_{\,i\,,\,p}-g(h^{\mu}_{\,i,\,p})]\ g^{|}(h^{\mu}_{\,i\,,\,p}) \qquad (8)$$

The weight from the input changes to hidden connection w_{d}, j, and k the rule is termed as delta rule and is applied to the indices, ΔI^{d}, j, and k are the processed image that contains medium resolution.

$$\Delta\ I^{d}_{j,\,k}=\acute{\eta}\ \sum_{\mu,q}\ \ \delta^{\mu}_{j,\,q}\,\text{€}^{\mu}_{\,k,\,q\,+\,t} \qquad (9)$$

$$\delta^{\mu}I_{\,j,\,q}=\sum_{S}\ g^{|}(h^{\mu}_{\,j,\,q})\ \sum_{i}\ \ \delta^{\mu}_{\,i,\,q\,-s}\,w^{s}_{\,i,\,j} \qquad (10)$$

Eq. (10) is the image that contains higher resolution.

A normal weight that contains bias b_i and b_j with invariable input to the layers and this total process contains the network training part. The testing process moves through the eq. (8), (9), (10) and the comparison is done to $\mu\ I_{j,q}$, $\Delta\ I^{d}_{j}$, and $\Delta\mu\ I_{i,p}$ of the input image in which if the three of the conditions are satisfying.

$$\delta^{\mu}I_{\,i,\,p}=[c^{\mu}_{\,i\,,\,p}-g(h^{\mu}_{\,i,\,p})]\ g^{|}(h^{\mu}_{\,i\,,\,p})$$

In which I^{1} resembles testing image and later the system will trigger to the server of storage for Homomorphic authorization.

B. Homomorphic Encryption within the Cloud

The input file f by the utilizer to the cloud through encryption algorithm and k as key and is defined as furnished below:

$$[[f]]=Enc(f,\,k)=f\ \oplus k \qquad (11)$$

[[f]] is the file that exists within the encrypted format and it is shared in the cloud architecture.

$$f=Dec\ ([[f]],\,k)=[[f]]\ \ \oplus k \qquad (12)$$

The encrypted file if downloaded should be decrypted and recouped to its basic or original form and it is carried out as below:

$$K=\sum_{i=0}^{m1}\binom{l}{i}\leq\frac{2l}{s}\leq\sum_{i=0}^{m1+1}\binom{l}{i} \qquad (13)$$

The '*k*' key is reduced by using the eq. (13) in which l and *i* are the facial features that are acquired from eq. (9), (10) in which we utilize S=2n which creates the derived keys from *Q0*, *Q1*, ..., *Qs-1*, and they are sizes *L*=MxNx8 bits. The different *Qj*'s for $0 \leq j \leq S$-1, are kept invisible by which the image features are hidden.

$$[f]=\sum_{i=0}^{m1}\binom{L-1}{i}\leq\frac{2l-1}{s}\leq\sum_{i=0}^{m2+1}\binom{2L-1}{i} \qquad (14)$$

The above furnished formulates are the fragmented file *[f]* that are structured within the cloud architecture in which the data that is existed in the fill is integrated as per the common data which is present within the file and is compressed to L-1 and 2L-1 in which I is the multiple of each occurrence of the data m_1 and m_2. Because the key is fed from the templates of the face, the key is then converted into a decimal or alpha decimal character.

C. Storage within Cloud

The storage within the cloud is defined as:

$$Li=(L!/i!(L-i)!) \tag{15}$$

Li is termed as the available size after the file storage within the configured cloud platform and L is the real-time size of the file and L! is the size of the file before the storage process. The I! is the multiplier in which the fragments of the file are processed and I is the sum of files that are processed at a time.

The following are the steps involved in the storage of file in the cloud:

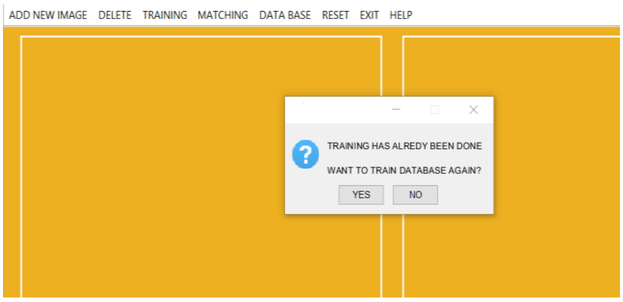
1) Starting of file block with a value of I=1
2) Focus n bits of a file to a confined location and is given by w_i
3) Determination of file location $Q[w_i]_d$ that is linked with w_i, $[F_i]_d$ = file itself, and W_i = descriptor index of the table of the file
4) The 'n' message length bits are embedded into $[F_i]$ in which the location is i^{th} block.

$$[[f]]_i^w = [[f]]_i\, Q[W_i]_d \tag{16}$$

5) $[[f]]\ w_i$ is the file that is stored within the cloud storage in which the modified input file $[[f]]$I and $Q[W_i]_d$ is the file location that is stored.

V. Test Results

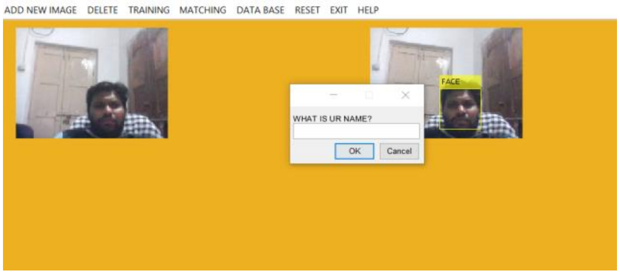
The procedure is performed on two servers that are capable of running the python platform for facial identification. The other abstraction added in this system is the cloud server as it allows the files that are encrypted and stored in the storage layer. The initial authentication part is triggered whenever the web app loads and the camera triggers at that particular point. The new utilizer to the platform is enabled with registration via the image capturing portal which is at the utilizer's disposal. The capture portal triggers the utilizer for the capture of the face. This process will go through different steps as furnished in Section IV.*A*. Depending on the face key point which is recognized from the image, the templates of the face are stored within the authorized server and the time is taken to perform these tasks like capture, identification and training is 15 seconds. The next process is cloud storage in which the utilizer acquires the file inputs of all the formats and can encrypt the files utilizing the facial key feature in which the input of the face is prompted during the process of encryption which requires a key. The facial key features are computed to acquire an integer value as furnished in Section IV.*B*. and it is important for the process of encryption. The files are then processed in the third-party cloud storage for storage purposes. The file downloading process is performed by another user and will be prompted for a facial key by which if the file belongs to the original owner and is decrypted and if not, the file becomes a non-utilizable entity. The important step in the complete process is the facial template and it plays a key role in the decryption or encryption of the file the aspect of accuracy also plays a key role. The total number of samples taken in this study is 100 and the rate of recognition is 95% and the balance is left for deviation. The total face samples that were exactly classified are 95-88 and classified are 100 by which the system accuracy is noted as 91% in the ideal condition scenario and 89% in the non-ideal condition scenario depending on the power of the system processing. The storage time taken is 0.01ms for 3kb.



TRAINING HAS ALREDY BEEN DONE

WANT TO TRAIN DATABASE AGAIN?

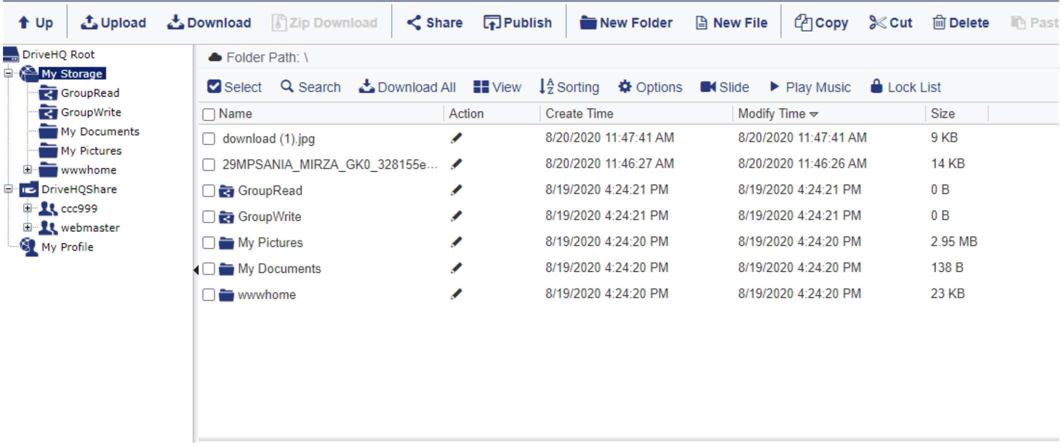
Figure 2. Training database.



WHAT IS UR NAME?

Figure 3. Users registrations.

Fig. 2 and Fig. 3 furnish the facial recognition interface for the web service of the facial authorization server within the cloud service and in this system, the images are converted into micro resolution as per the concept of CNN and these are discussed by utilizing the Eq. (3) & (4). The images are then processed into the maximum pooling layers which are discussed in Eq. (5) and (6). The output layers are then utilized to store the image in a binary form and a duplicate of the image is described in Eq. (7), (8) and (9) this complete process consists of training with the facial database that is created. The utilizer after completing the registration process will sign in to the account in which the user facial input is taken so that the output layers will be triggered as discussed above and the matching of a face by the facial database is processed and the face is identified and utilizer will be authorized into the cloud service. The utilizer will be furnished with an uploading facility in which the utilizer should go through a process of encryption and it is a compulsory one. During this process, the utilizers are prompted with the facial input from the camera by which the utilizer image is converted into the key depending on Eq. (11), (12), and (13). The final output is an image key that is utilized for the file encryption which has to be uploaded within the cloud as furnished in Fig. 4.



☐ Name	Action	Create Time	Modify Time	Size
☐ download (1).jpg	✎	8/20/2020 11:47:41 AM	8/20/2020 11:47:41 AM	9 KB
☐ 29MPSANIA_MIRZA_GK0_328155e...	✎	8/20/2020 11:46:27 AM	8/20/2020 11:46:26 AM	14 KB
☐ GroupRead	✎	8/19/2020 4:24:21 PM	8/19/2020 4:24:21 PM	0 B
☐ GroupWrite	✎	8/19/2020 4:24:21 PM	8/19/2020 4:24:21 PM	0 B
☐ My Pictures	✎	8/19/2020 4:24:20 PM	8/19/2020 4:24:20 PM	2.95 MB
☐ My Documents	✎	8/19/2020 4:24:20 PM	8/19/2020 4:24:20 PM	138 B
☐ wwwhome	✎	8/19/2020 4:24:20 PM	8/19/2020 4:24:20 PM	23 KB

Figure 4. Cloud encrypted files.

TABLE I. TIME TAKEN FOR TRAINING PROCESS

S.No	Algorithm	Speed of Training (Sec)	Speed of Storage (ms)	Speed of Recognition (ms)	Efficacy (%)
1	SVM	30	0.9	100	76
2	Bayesean Classifier	45	0.5	150	73
3	ANFIS	25	0.2	70	78
4	CNN VGG-16	18	0.14	40	87
5	CNN VGG-19	15	0.01	20	89

The cloud images are downloaded apparently and should be decrypted by the utilizer. To decrypt the file, the utilizers are prompted with the camera input by which the facial information is compared and if the authorization is passed then the file is decrypted or else it will be a failure task as furnished in Eq. (14). The whole process enables and ensures the complete privacy of the utilizer and their uploaded files, as the individual utilizer will have complete copyrights of the uploaded content. Table I furnishes the comparison of time taken for the process of training and different parameters of the complete process and their time of processing.

From Table I, it is evident that by utilizing the proposed method, the improvement aspect in every attribute is identified within the cloud storage system which utilizes different algorithms.

VI. CONCLUSION

The present study has recognized an alternative authorization system within the cloud architecture by utilizing face key vector points and the efficacy by using CNN is enhanced from 75-90% and the time of storage is enhanced from 0.15ms to 0.01 ms for 3kb. The system of capture that is furnished in this study utilized the commodity hardware for the complete process and this aspect enhanced the cost efficacy of the deployment of the model. The third-party server is the customized cloud that is created for the ideal conditions and it is allocated with unlimited storage resources to enable files of various kinds and sizes. Persons of various ages are also tested for recognition efficacy. The complete process is expected and concluded to be an alternative effective methodology for the privacy protection of the user within the cloud platform. The outcome and major contribution of the study are providing safety and security to the information which is stored within the cloud platform effectively.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Tadi Chandrasekhar has performed all the research studies and Sumanth Kumar has monitored and mentored the complete research study; all authors had approved the final version.

REFERENCES

[1] C. Wang and H. Yan, "Study of cloud computing security based on private face recognition," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 2015.

[2] F. A. Silva, P. Maciel, E. Santana, *et al.*, "The model of face recognition in video surveillance based on cloud computing," *Computing*, vol. 99, pp. 287-311, 2017.

[3] Y. Zhu, Z. Huang, and T. Takagi, "Secure and controllable k-NN query over encrypted cloud data with key confidentiality," *J. Parallel Distrib. Comput.*, vol. 89, pp. 1-12, December 2019.

[4] Y. Li, S. Wang, Y. Zhao, *et al.*, "Simultaneous facial feature tracking and facial expression recognition," *IEEE Transactions on Security Systems*, 2019.

[5] Y. Sun, J. Zhang, Y. Xiong, *et al.*, "Data security and privacy in cloud computing," *International Journal of Distributed Sensor Networks*, July 2014.

[6] L. Verderame, I. Merelli, L. Morgantic, *et al.*, "A secure cloud-edges computing architecture for metagenomics analysis," *Future Generation Computer Systems*, vol. 111, October 2020.

[7] S. N. Srirama, C. Paniagua, and H. Flores, "CroudSTag: Social group formation with facial recognition and mobile cloud services," *Procedia Computer Science*, vol. 5, 2011.

[8] A. Vinay, A. Joshi, H. M. Surana, *et al.*, "Unconstrained face recognition using ASURF and cloud-forest classifier optimized with VLAD," *Procedia Computer Science*, vol. 143, 2018.

[9] D. K. Jain, P. Shamsolmoali, and P. Sehdev, "Extended deep neural network for facial emotion recognition," *Pattern Recognition Letters*, vol. 120, April 2019.

[10] M. Masud, G. Muhammad, H. Alhumyani, *et al.*, "Deep learning-based intelligent face recognition in IoT-cloud environment," *Computer Communications*, vol. 152, February 2020.

[11] A. K. Jain, S. Pankanti, S. Prabhakar, *et al.*, "Biometrics: A grand challenge," in *Proc. 17th IEEE Int. Conf. Pattern Recognition*, 2004, pp. 935-942.

[12] V. A. Bharadi and G. M. DSilva, "Online signature recognition using Software as a Service (SaaS) model on public cloud," in *Proc. IEEE Int. Conf. Comput. Commun. Control Automation*, 2015, 65-72.

[13] S. Guo, T. Xiang, and X. Li, "Towards efficient privacy-preserving face recognition in the cloud," *Signal Processing*, vol. 164, November 2019.

[14] P. Hu, H. Ning, T. Qiu, *et al.*, "A unified face identification and resolution scheme using cloud computing in Internet of Things," *Future Generation Computer Systems*, vol. 81, April 2018.

[15] K. Sun, H. Kang, and H. H. Park, "Tagging and classifying facial images in cloud environments based on KNN using MapReduce," *Optik*, vol. 126, no. 21, November 2015.

[16] H. Debnath, M. A. Khan, N. R. Paiker, *et al.*, "The Moitree middleware for distributed mobile-cloud computing," *Journal of Systems and Software*, vol. 157, November 2019.

[17] J. Zeng, C. Li, and L. J. Zhang, "A face recognition system based on cloud computing and AI edge for IoT," in *Proc. International Conference on Edge Computing*, June 2018.

Tadi Chandrasekhar received the AMIE degree in ECE from The Institution of Engineers, Engineers (India) and an MS degree in Embedded Systems from Manipal University, He Currently Pursuing a Ph.D. in Image processing from GITAM University, India. He currently working as Professor& HOD at ISTS Women's Engineering College. He has 22 years of experience in teaching and 7year research experience in Image processing, Deep Learning & Cloud Computing, etc.

Sumanth Kumar has done Ph.D. from Andhra University, India. He currently working as an Associate professor at GITAM University. He has 18 years of experience in teaching and 10year research and published 17papers in high indexed journals. He published two books on signal processing.