International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209697 Volume 8, Issue 4, July – August (2021)

RESEARCH ARTICLE

Enhancing Security of Cloud Data through Encryption with AES and Fernet Algorithm through Convolutional-Neural-Networks (CNN)

Pronika
Department of Computer Science and Engineering, Faculty of Engineering and Technology, Manav Rachna International Institute of Research & Studies, Faridabad, Haryana, India.
pronikachawla123@gmail.com

S.S.Tyagi
Department of Computer Science and Engineering, Faculty of Engineering and Technology, Manav Rachna International Institute of Research & Studies, Faridabad, Haryana, India.
shyam.fet@mriu.edu.in

Received: 08 May 2021 / Revised: 30 June 2021 / Accepted: 11 July 2021 / Published: 28 August 2021

Abstract – Cloud as a storage in the recent technological development had been focused by researchers, since it offers more insight towards meta-data based security and safety along with techniques in encryption and decryption of messages. "Data" being a crucial and complicated means-of-information in current technological era, it has been majorly accessed and utilized for varied purposes (example: image storage/access) by people globally through 'cloud computing' via social platforms, personal data-storage, professional data-accumulation, research based studies, etc. Thus to protect data in cloud, especially the images, the current study developed the algorithm by combining 'AES' and 'Fernet' where double-level encryption with CNN Auto-Encoders. Thus by developing the model, the study aims to provide more secured cloud computing model than existing models. The original images as input are processed, encrypted/decrypted, converted into bitmap images as outputs that are decrypted by users with 'key' when needed. The study was a success and found to be effective in image encryption field with high RMSE (0.040206), less MSE-Loss (0.001616) and MAE (0.0266323) scores than estimated scores.

Index Terms – Cloud Computing, Face Images, AES Algorithm, Fernet Algorithm, Data Security, Data Safety, Data storage.

1. INTRODUCTION

The data as source for many researches and studies is considered as the "new black-gold". In many countries currently the impact of pandemic situation had made the researchers seeks for storing, accessing and modifying data as per their necessity. However the security and safety standards of the meta-data especially in the cloud are at tremendous risk, where, data theft, data manipulation, data falsification and misinformation are at large. Hence securing the data in cloud and encrypting the information or messages have been recently focused by researchers. In this study the cloud computing and securing the information, "face images" is focused, where a model is developed with CNN embedded with Auto-Encoder where encryption and decryption of face images is particularly focused.

Data storage in the cloud is witnessed as a risky option for high-level confidential information and personal information that could get the user to experience data loss, data theft, data manipulation and data forging [1]. Though there are challenges and risks in cloud computing it is the permanent solution for the meta-data users and seekers. Meta-data in cloud servers are mainly accessed and stored by varied people globally based on cost/ budget, time, space and access across longitudinal location [2]. Henceforth many private and public servers based cloud computing have been criticised towards poor security and safety of information leading towards many data manipulation. Thus researchers and algorithm developers in par with Government had compiled many safety and secure ways of data in cloud computing where: the restrictions of locations, encryption and decryption, security based questions, symmetric and asymmetric key based numerous encryptions [3]. [4], [5] Data security and data storage based safety is quite complicated in the public servers unlike the private and hence encryption at user end prior sending the information to receiver or storing the information in the cloud is essential which is reliable, cost effective and secure unlike maintenance fees in private clouds and storage access cost.

Encryption in cloud computing especially the image and text encryption in the current technological advancement had been recognised and adopted by many organizations to prevent data theft and data loss during data transmission that are highly confidential [6]. Similarly techniques like AES, Hash function, Symmetric and Asymmetric key functions, SKM, Hill Cipher and Chaotic-Logistic Maps, etc have been studied by researchers [7], [8], [9] Image encryption than text encryption. Though the image encryption is done through cryptography techniques, the performances of each technique vary as per the inputs and variables along with the attributes of the images as inputs and purposes of researches. Generally face recognition studies, gender recognition, age discrimination based studies and ethnicity based studies had been conducted more in the research field the lack of image encryption in cloud computing towards social media and personal storage have been identified recently, since the data storage and access in the recent years after pandemic situations have heightened. However the issue of data storage in cloud computing as face images being inputs has never been attempted through hybrid algorithm. [10] had attempted to encrypt images in clouds through 'Chaotic maps' and stated that image encryption is quite easier to encode and decode than plain texts since they deal with RGB-colours and attributes like: illumination, gradient, contrast and size as variables.

The uses and adoption of data storage and data access in cloud computing according to authors [11] mainly focuses on *virtualization* where government organizations, commercial companies and IT people are the most witnessed users. However the same view was contradicted by the authors [12], [13] stating that normally people of varied gender, age, occupation and ethnicity, globally utilize the cloud servers to store and access data through cloud-service providers and private cloud servers unlike those who can access and store data (text and images) through public servers and face data security based issues than private cloud computing.

Though cloud computing based researches are normally focused through personal computers, laptops and official computers, mobile as a medium for cloud computing is also facing a surplus issues where data security and data storage collides due to minimal data storage (disk/ memory space) and exposes the users towards cloud computing [14]. However there are options for mobile cloud-computing where security could be tightened with two-or-more bio-metric access (voice/ fingerprint/ password/ face recognition). These bio-metric based access for cloud computing and storage could be categorized as data encryption and cannot be categorized as image encryption. Image as security based encrypted or ciphered blocks in the clouds have been analysed and studied [15] where it was stated that in image encryption hybrid algorithms for encoding and decoding is an efficient technique unlike the single level encryption that could be easily breached or hacked. Preserving privacy especially with image encryption/decryption in cloud computing is mostly effective with AES algorithm [16] where AES is standard algorithm and mostly utilized for image encryption/decryption in US. Securing data in cloud computing through image searching and image storing is crucial since it protects data as "black box", i.e. the control upon the users' data is lost once the data had been stored in the cloud [17] hence encrypting each image prior storing through AES, Hyper Chaos, Cipher encryption, etc are recommended however single level encryption as plain text or cipher text could be manipulated or forged once the key has been illegally or maliciously obtained by the hacker/ third parties [18]. Henceforth developing a encoder/decoder model with CNN or ANN through hybrid algorithm adoption where the level of encryption is higher and meticulously planned towards decrypting and retrieving the data (images) with lesser noise and minimal to zero data loss should be the primary focus of a researcher since there are other existing researchers where image encryption mainly focuses on single level encryption [19], minimal data loss [20] and cloud computing in mobiles [21] etc.

Thus the primary focus of the proposed research would be upon the cloud computing and its security in image storage through encoder/decoder model developed through AES algorithm and Fernet algorithm as hybrid in double-level encryption/decryption where the CNN is adopted with the Auto-Encoder training of datasets in the deep learning. The research also thus offers and contributes information towards Fernet and AES as hybrid technique in securing the data in cloud computing through face images as inputs rather than text as inputs. Datasets would be acquired and cleansed prior training and applying the algorithms. Through this research, future researchers would also gain insights of comparative analyses of Fernet with AES and other hybrid image encryption in cloud computing.

1.1. Organization of the Paper

The section 1 of this paper explains the background of cloud data and section 2 is the literature review followed by the research gap. Section 3 explains about AES Algorithm and section 4 explains about FERNET algorithm. In section 5, proposed methodology and Model development is explained. Section 6 has the results and discussion. Finally section 7 has the conclusion of the paper.

2. LITERATURE REVIEW

2.1. Data Security

According to their study the client and the receiver side in cloud computing are both at risk in transmitting and receiving information and henceforth to provide security and services the authors had developed a flexible scheme of distribution where the user would be able to store data and access data remotely. Through remote access in cloud computing the user would be exposed to lesser risk and data theft unlike the shared access.

Similarly the authors [4] has also analysed the data security and storage in cloud computing where the common occurrences of data theft, data breaches and cloud data unavailability are examined and analysed. As per their findings the study concluded that (i) cloud storage based issues are normally found with: data integrity and privacy, data vulnerability and recoverability, inappropriate media refinement and data backup issues; (ii) access control issues and identify mismanagement are found through: outside intruders and malicious insiders; (iii) legal and contractual issues are identified through: illegal access/ manipulation and SLA. Thus the study has argued that data security and storage are the most concerned issue in cloud computing.

In the study by [5], it has been found that cloud computing and data storage has been witnessing huge issues towards data security and data storage especially with images as storage. Henceforth the author developed a POR algorithm along with DSBT scheme towards identifying the inputs and encrypting the inputs through ciphering (signcryption) to attain efficient model towards encryption/decryption of private data in cloud computing and cloud storage. The author also utilized the time encryption along with the DHT network towards heightened security of data storage and data access.

2.2. Image Encryption / Decryption

A new technique towards image encryption through Henon chaotic-map and tested the developed model through progression of tests for measuring the performance metrics [10]. Through the examination and evaluation the authors found that the developed algorithm was recorded as highly sensitive against the statistical attacks and varied brutal-forces. The study utilized the vertical and horizontal permutations based matrix and pixel shuffling as secret key.

The authors [9] examined and researched digital image based encryption algorithm through double logistic chaotic-map. The authors aimed at examining the data theft and developed their model towards identifying the attacks through third-party and hackers and to prevent data theft and loss. The tool adopted by the authors were the dual-logistic based chaotic-map since it offers randomness in cipher-text towards making the deciphering pretty easy and rapid unlike other methods. Simultaneous experimentation was done upon the chosen inputs and the research concluded that the method adopted was efficient when compared against other techniques.

2.3. Cloud Computing

Authors [11] had surveyed the existing challenges in cloud computing and examined the security issues and safety measures in virtualization. According to the studies' surveyed findings virtualization being the new trend for the current generation has been targeted by the third parties to interfere with transmissions of files and information and cloud data accesses. Henceforth the study surveyed the stakeholders and the investors in the cloud computing towards vulnerabilities in virtualization and concluded that secure cloud computing has been offered by private service providers through remote access and encryption based algorithms that prevents the third party interferences and improves security in data storage and access.

Recently the researchers [13], [20] and [14] had studied about the security based challenges, risks, taxonomy and architecture in mobile and computer cloud computing. According to their findings though there are several security based options offered by the cloud service providers and algorithm developers the hackers and third-parties are increasingly advancing in their ways to penetrate through the fire-walls and security in cloud to obtain confidential information. Henceforth the cloud computing based industries have been severely hindered and thus the challenges still persists which makes the users to lose data or information that they store in clouds. The authors concluded in their study that, architecture and taxonomy of the cloud makes the third-parties to penetrate the clouds easier to obtain confidential information and thus the solution lies in altering the architectural approach; similarly the users should opt for remote access through double-level encryption which could protect their data like adopting two-or-more hybrid algorithm in encoding/decoding.

2.4. Image Encryption / Decryption in Cloud Computing

Studies in 2019 by authors [17] focused on image encryption and secure ways to protect data storage; similarly authors [16] had also focused on cloud storage and privacy preservation but in mobile cloud. However both studies found that the users store huge images in clouds and access or retrieve with risk of data exposure and theft. The studies found that, Chaotic maps, Fernet and AES algorithms are being adopted by the developers to prevent images through encryption/decryption models and thus they argued and concluded by stating that encrypted images should be done through secured and reliable encrypt/decrypt model prior storing the data in the clouds and while retrieving users should opt for remote access which would offer the users with secured data and access.

Studies like comparative analyses by the authors [21] increased security and secrecy in data storage in clouds by [18] provides insights such as, cloud computing being exposed to vulnerabilities and risks especially with images in clouds than texts are increasing rapidly. Henceforth to provide secure storage along with safer access, traditional algorithms like AES, DES, 3DES, RSA, BLOWFISH along with contemporary techniques should be combined as hybrid algorithms with complex neural networks which would hinder the third-parties and their efforts at data theft.

2.5. Research Gap

Thus it could be inferred from the reviews that, algorithms in cloud computing and cloud storage should be adopted to prevent data theft especially towards image as inputs through encryption / decryption model where the neural networks should be complex and algorithms should be hybrid to ensure higher security and efficiency unlike single-level encoding/decoding. It is also inferable that image encryption/decryption in clouds should be carried prior storing the data rather than applying security within clouds, thus preventing data forging or data manipulation and image loss.

The proposed algorithm in image securing through encryption and decrypting model consists of two algorithms (i.e. hybrid) where the AES (Advanced Encryption Standard) or Rijndael algorithm along with the Fernet algorithm as techniques have been adopted. Thus the research fills existing literature gap by developing a new model by combining the basic and advanced algorithm (AES & Fernet) as the first model and compare the outcomes with estimated outcomes.

3. AES ALGORITHM

The AES algorithm is the most standard and trusted algorithm for encryption especially in image encryption where the key is generated, 128bits is modified into 16/ 32/ 64 bits for rapid processing of blocks and balanced loading [22]. The proposed research developed an AES algorithm based on the following steps:

3.1. Encryption / Decryption

Step 1: Key generation: Initially set-of-round keys are gained from the Cipher key;

Step 2: Initialization of the state array is applied upon the plaintext / block array;

Step 3: Next, the primary round - key is added to the initialized state array;

Step 4: Next, state manipulation of nine rounds is performed;

Step 5: Finally the tenth state manipulation round is performed prior acquisition of cipher text;

Step 6: Lastly the final - state array acquired is copied as the obtained ciphered - text / encrypted data

Thus the encryption is carried out where the 128bits sequence is converted as 16bytes for AES since it performs well as 16bytes. For the decryption the inverse functions (InvSubBytes, INVShiftRows, INVMixColumns) will be carried out where:

Step 1: Initial decryption round is performed;

Step 2: Nine-full decryption rounds are followed

Step 3: Finally the Xor Roundkey is performed to decrypt the cipher text.

Thus the algorithm is developed and applied upon the datasets to train and test the accuracy of the developed encoding and decoding rounds in AES.

3.2. Advantages / Disadvantages

Implementing the robust-security based symmetric AES algorithm in software/hardware is easier, resilient towards hacking with key sizes that are long (i.e. high-length), open-source, most commonly adopted and utilized.

However when adopted/utilized on Solid-State-Drives (SSDs) it’s identified as less foolproof and thus adopting hybrid model is recommended for confidential datasets.

4. FERNET ALGORITHM

Similar to the AES algorithm the Fernet also uses plain-text as ciphering/ encrypting but the difference lies in the process of the algorithm where Fernet provides the rotation of keys generated through “MultiFernet” [23].

4.1. Encryption / Decryption

Step 1: Generate the key;

Step 2: Assign the key value to the selected variable;

Step 3: Convert the plain-text into a ciphered-text;

For decrypting the encoded text, the conversion of cipher-text to plain text in Fernet is carried out as inverse function and the output is displayed as “string” value from bytes.

4.2. Advantages / Disadvantages

The benefits include, sign-stamping (signature through SHA256 and HMAC), time-stamping, random allocation of “salt values” for security, generation of key through secure mechanism and adopting secure algorithm towards encrypting messages (PKCS7 padding and AES under CBS-mode) that offers high encryption where data-manipulation is impossible without key.

The key disadvantage is that, the key could be obtained by third-parties while transferring to the receiver’s end which is highly-risky and a huge drawback in Fernet and other symmetric cryptography.

4.3. Rationale for AES and Fernet Adoption

Though there are other symmetric and asymmetric algorithms for en/decryption the AES is commonly adopted and standardised algorithm and whereas Fernet provides users with more secured key that lacks in the existing symmetric algorithms. Thus by combining AES with Fernet the study aims at high-level en/decryption of images as inputs in CNN based En/Decoder model which has not been attempted prior in existing studies.

5. PROPOSED ALGORITHM AND MODEL DEVELOPMENT

The study developed the double encryption method through the CNN where the auto-encoder is utilized. The main purpose of adoption of auto-encoder is to minimize and ignore the "noise" through training since the proposed research makes use of images as inputs, face images in encoding and decoding. In cloud computing data, especially the personal information is highly at risk and thus securing the face images in clouds is essential through encryption and decryption process. The developed hybrid algorithm of Fernet with AES offers double-level encryption/decryption technique.

5.1. Proposed AES Encryption Algorithm

The AES algorithm developed here offers the researcher with standard algorithm and the datasets are trained and tested through the developed model. The key is expanded and round-key is added primarily, later storage area is stated and the functions of ByteSub, ShiftRow and MixColumns are carried out (refer Figure 1). The steps are repeated until the encryption or ciphered text is obtained and saved. Once the ciphered text is attained, it is attached to the original input and sent to the receiver where the decryption takes place as inverse function. The AES is most trusted algorithm that offers the researchers with trustable encryption especially with Auto-Encoder based CNN the AES with Fernet is aimed to be effective and complicated for data forging and manipulation when accessed by hackers or third parties.

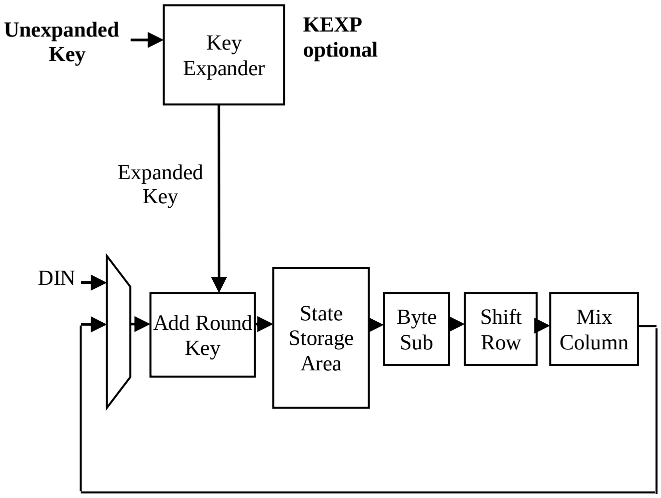


Figure 1 AES Algorithm

In the double-level encryption *"b"* is added as round-key and through output of the encryption it could be seen that *b* is appended with the original image, through double-level decryption the original input as variable is obtained with pre-defined block-size for the images.

5.2. Proposed Fernet Encryption Algorithm

The Figure 2 represents the Fernet symmetric encryption where the key is generated through custom derivation key-generation function by adopting the source codes of PBKDF2 and KDF.

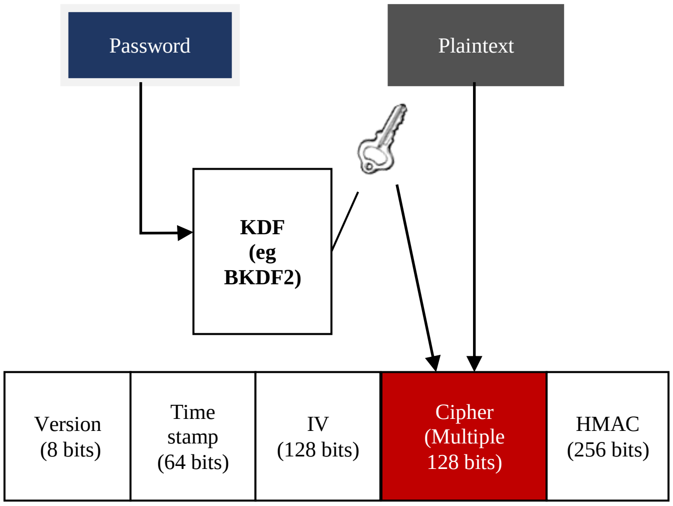


Figure 2 Fernet Algorithm

"Generated Fernet Key = phJnZmXUMoe57l20jdwY7NbDmdsaCQCWAq8lc6dtEvQ="

The key is of plain text password with 128bits ciphering. In this level the trained datasets are encrypted at first level in Fernet and applied on the data-input images through the Auto-Encoder and developed CNN. Once the images are encrypted they are then passed on to AES encryption where second level encoding takes place.

5.3. Proposed System-Flow

The proposed method has two sets of pipeline where sender and receiver have different stages in processing the images (refer Figure 3).

Through the above pipeline diagrammatic representation the processes are explained individually and thus the flow of the proposed model could be deduced as (refer figure 4) a single project flow representation:

Thus it could be understand through the proposed model that, through double level encryption and CNN the model is trained with datasets performing with Auto-Encoder where the desired outcome is compared with original outcome for reliability and accuracy of the developed model. The performance evaluation would be weighed through MSE, RMSE and MAE scores and the model would be weighed for accuracy and reliability through the scores of performance of the encoder-decoder model.

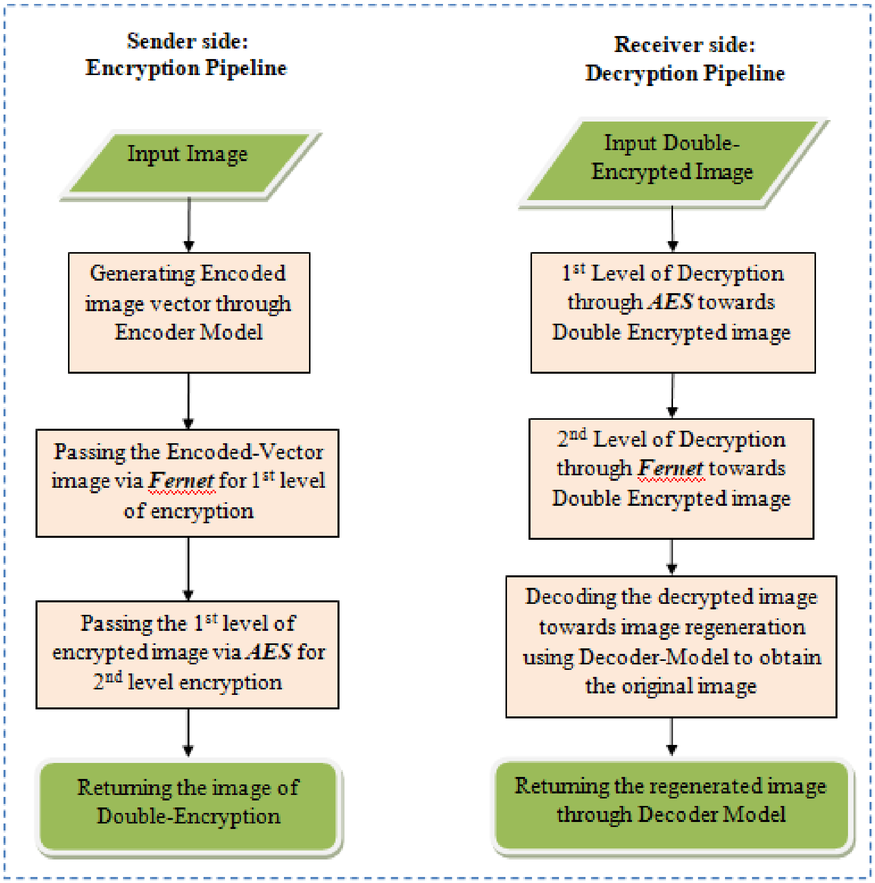

Sender side:
Encryption Pipeline
Input Image
Generating Encoded image vector through Encoder Model
Passing the Encoded-Vector image via Fernet for 1st level of encryption
Passing the 1st level of encrypted image via AES for 2nd level encryption
Returning the image of Double-Encryption
Receiver side:
Decryption Pipeline
Input Double-Encrypted Image
1st Level of Decryption through AES towards Double Encrypted image
2nd Level of Decryption through Fernet towards Double Encrypted image
Decoding the decrypted image towards image regeneration using Decoder-Model to obtain the original image
Returning the regenerated image through Decoder Model

Figure 3 Pipeline Diagram of the Proposed Model

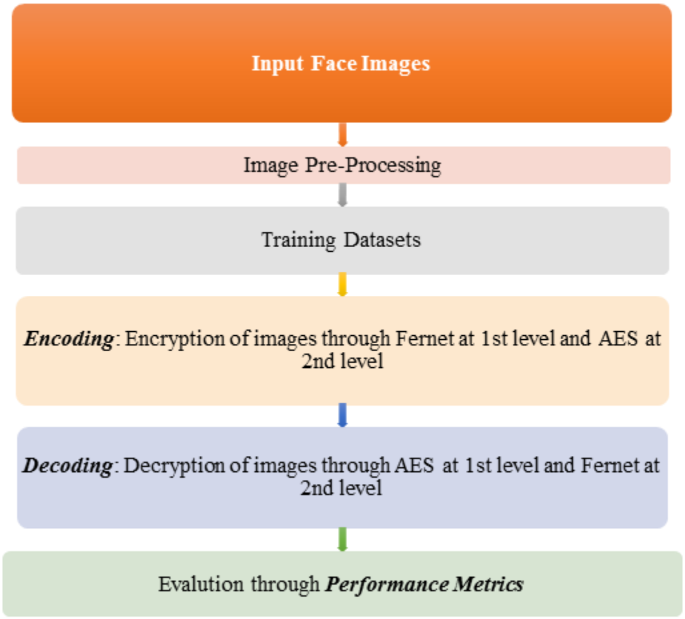

Input Face Images
Image Pre-Processing
Training Datasets
Encoding: Encryption of images through Fernet at 1st level and AES at 2nd level
Decoding: Decryption of images through AES at 1st level and Fernet at 2nd level
Evalution through Performance Metrics

Figure 4 Proposed Model Flowchart

5.4. Auto-Encoders in CNN

The CNN based Auto-Encoder is generally designed towards reducing the noise in the images. In this proposed research the parameters are *Conv2D, Dense, Input, MaxPooling2D, UpSampling2D* and *Conv2DTranspose*, where the input of original image is flattened and passed through the bottlenecked-coding (encoding) and then later on the flattened image is retrieved as reshaped image with reduced noise (decoding) as bitmap output.

The approach utilized here would be basically through double encryption which is developed through the following steps:

Step 1: Initially the Auto-Encoder in CNN (Encoder-Decoder Model) is trained towards encoding (encrypting) and decoding (decrypting) the images as inputs;

Step 2: The encoding of the images is done through double level encryption where the images are passed via two-level encryption techniques prior processing and decoding;

Step 3: The first level is the Fernet-level encryption and the second level is the AES-level encryption

Step 4: Once the image is encrypted, it is regenerated through two-level of decoding, i.e. the encrypted image would be regenerated as vector in first-level decoder and into bitmap as original image in the second-level of decoder.

5.5. Research Datasets

The datasets for the research is obtained from the UTK Face-Dataset bank from the link: https://www.kaggle.com/abhikjha/utk-face-cropped

The obtained datasets is a meta-data based datasets with age span ranging from 0-116yrs old. It is of large-scale dataset especially stores only the "face datasets" as inputs for examination and research purposes. Generally the databank contains 24,000plus face-images which have huge range of race, gender, age, ethnicity, etc; which also focused on variations like: facial expressions, occlusion, poses, resolution, illuminations and so on. The images are well-cropped, dimensioned and aligned for researches. Though the datasets are generally utilized for researches to determine face detection based studies, age estimation/regression/progression based researches, etc. Justification of dataset adoption: Researches like the current study is also valid and justified to utilize these datasets since they offer accurate information with well-focused through encoding and decoding face images as inputs for researches. Authors [24] had adopted the face datasets in determining the alterations of gender and ethnicity and found the inputs and estimated outcomes reliable.

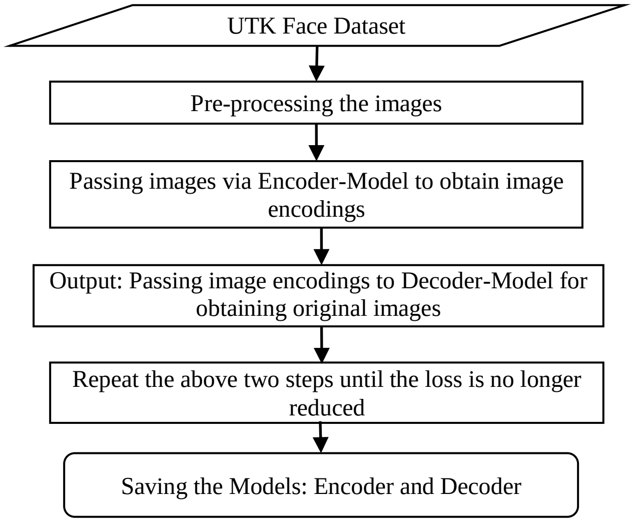

UTK Face Dataset
Pre-processing the images
Passing images via Encoder-Model to obtain image encodings
Output: Passing image encodings to Decoder-Model for obtaining original images
Repeat the above two steps until the loss is no longer reduced
Saving the Models: Encoder and Decoder

Figure 5 Training Dataset Flow Diagram

5.6. Encoder Model Architecture

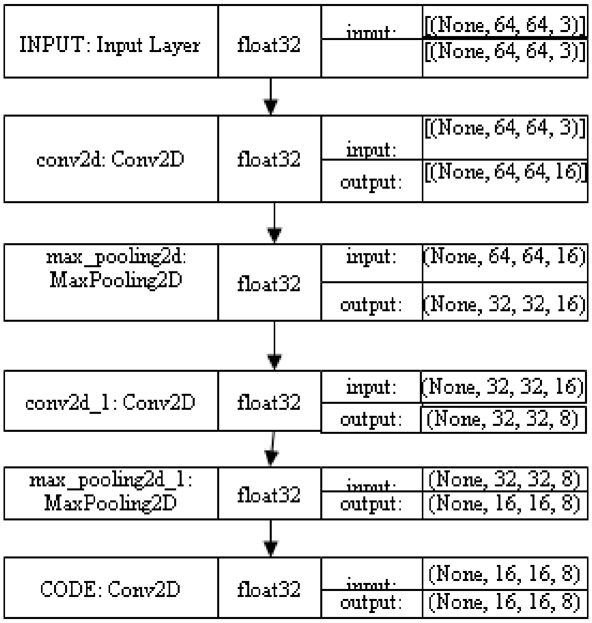


Figure 6 Encoder Model

The CNN (Convolutional Neural Networks) in the deep learning is generally described as a class belonging to deep NN towards analysing the visual imagery with hidden layers and kernels [25]. Based upon the CNN based fully connected 'multilayer perceptrons' networks, the encoder and decoder architecture model have been developed. The encoder model (refer Figure 6) developed here has double-level encryption.

5.7. Decoder Model Architecture

Similar to the developed encoder neural network, the decoder model (refer Figure 7) also works upon double-layer decryption where the images are decoded as vector images initially and the outcome as original images.

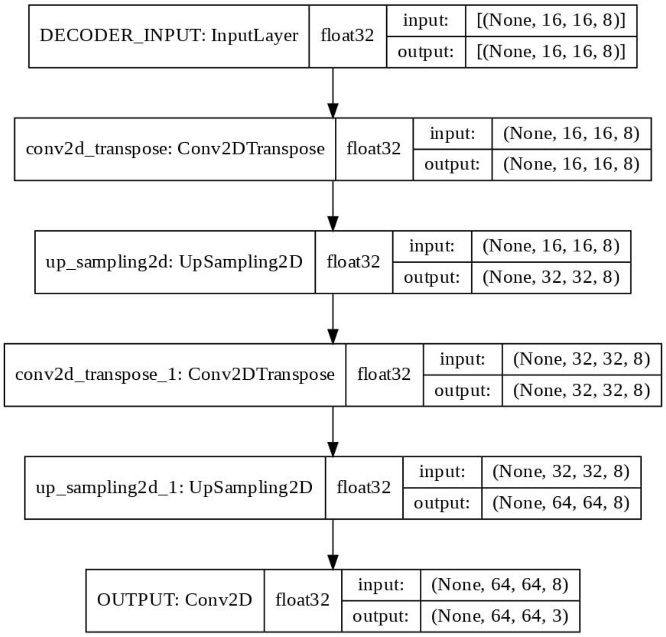


Figure 7 Decoder Model

5.8. Adopted Statistical Techniques

A research will be based upon numerical and statistical analysis when the estimated value/ outcome should be compared against the developed model. Likewise, in this research the following statistical formulae and techniques have been adopted and applied:

5.8.1. Sigmoid Activation - Functions

The sigmoid activation-function in the statistical evaluation analyses is also identified as standard logistic-function [26]. Generally the sigmoid function is characterized as:

$$(\boldsymbol{z}) = \frac{\mathbf{1}}{\mathbf{1} + \boldsymbol{e}^{-\boldsymbol{z}}}$$

The sigmoid function of logistic in NN of the deep learning is represented (refer Figure 8) through a graph plot, where commonly the x axis represents the values from -1 to +1 and whereas the y axis represents 0 to 1. Generally the sigmoid function is "s" shaped-curved where both axes meet at the points 0.5 of y and 0 of x.

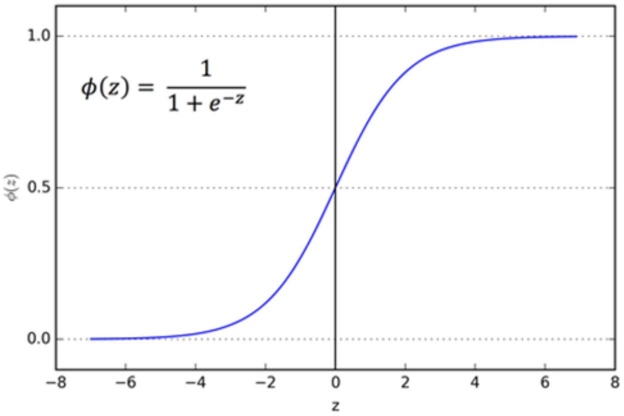


Figure 8 Logistic Sigmoid-Function Plot

The Nwankpa et al., had analysed about variations and classifications of deep learning activation functions and pointed out that the Swish AF (sigmoid function) outperforms the ReLU function in DL classifications. Thus the research aims at obtaining the smooth, unbounded upper-limits, bounded lower-limits and non-monotonic functions in the developed model of encoding and decoding.

5.8.2. ReLU Activation-Functions

The authors [27] and [5] had defined the DL and ReLU function in their research as a "trendy AF" that is being adopted and utilized by researcher for NN based studies. The ReLU is identified as piecewise function where the output is forced as "zero" when the input ≤ 0 (refer Figure 9); if not the outcome will be identical to the input variable.

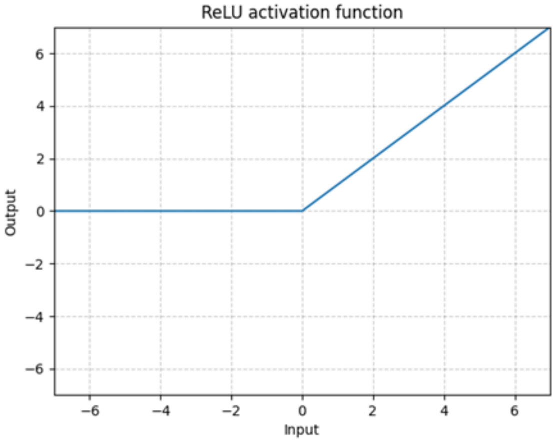


Figure 9 ReLU Graph Plot

The ReLU graph plot is mostly adopted for positive inputs where gradient diffusion issues are null unlike Sigmoid; whereas mostly ignored for negative value based studies since it offers the researchers with neuronal necrosis however it is adopted for its rapid computing rate. Hence, for face images as inputs ReLU AF is suitable with its attributes for computing along with Sigmoid towards faster computing and accuracy.

5.8.3. MAE

The MAE (Mean Absolute Error) is the observed pair's error measures which expresses identical phenomenon. Thus to measure the continuous variables' accuracy in this research MAE is adopted. Generally estimated by the following formula:

$$\mathbf{AE} = \frac{\mathbf{1}}{\mathbf{n}}\sum_{\mathbf{j=1}}^{\mathbf{A}} |\mathbf{a_j} - \hat{\mathbf{a}}|$$

5.8.4. RMSE

The RMSE loss value is calculated through the square root of the MSE value:

$$\sqrt{\mathbf{MSE} = \frac{\mathbf{1}}{\mathbf{n}}\sum (\mathbf{a} - \hat{\mathbf{a}})^{\mathbf{2}}}$$

The above are the analyses techniques and methods adopted for the research along with the numerical evaluation techniques.

6. RESULTS AND DISCUSSION

6.1. Results

The inputs in this research were selected 10images from UTK face images that are pre-processed and cleansed for processing.

The Table 1 represents the processes for the developed model where the input images are encoded and passed through CNN for encryptions i.e. encrypted via double encryption through Fernet as initial encryption and AES as secondary encryption level. Latter the images are retrieved via decoding algorithms (reversal) where the AES algorithm is primary decryption technique to obtain the vector images and the Fernet algorithm to obtain the original images through coding.

Finally the outcome/ outputs are obtained as bitmaps with 64*64sized in this research through the developed Auto-Encoder and Decoder model.

MSE Loss: The figure 10 represents the MSE Loss where the x axis is total Epochs and y axis is the loss.

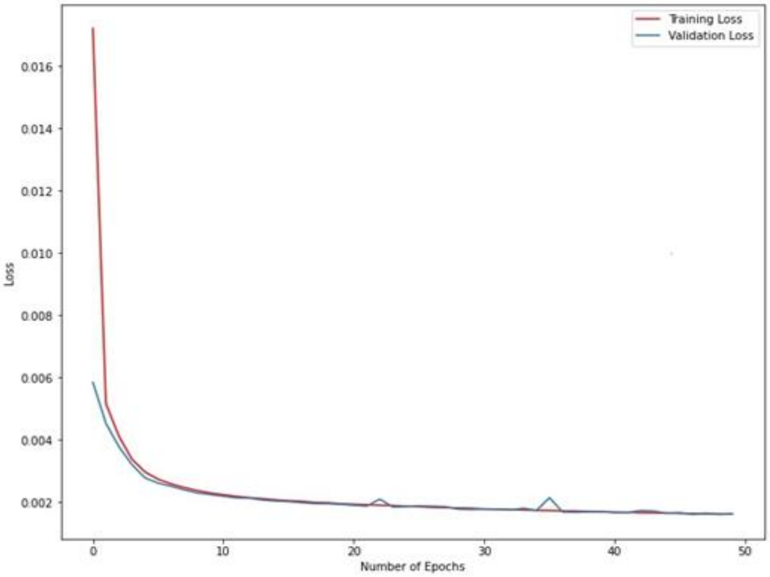


Figure 10 MSE Loss

Inference: The Figure 10 depicts the loss where the orange-line indicates the training loss and the blue-line indicates the validation loss. It could be clearly inferred that loss during the training was higher at zero and reduced at 50; whereas the loss during validation at the zero was comparatively lesser than training loss and reduced at 50 showing that loss has reduced gradually as the interval increased.

6.2. Performance Evaluation

The evaluation of performance metrics has been carried out through assessing the MSE, MAE and RMSE (refer Figure 11) values. According to the obtained outcomes and analyses it could be understood that performance metrics.

Inference: The Figure 11 represents the scores of the developed model through statistical evaluation. According to the obtained outcome it could be inferred that, the MSE score is 0.001616, RMSE score is 0.040206 and the MAE score is 0.0266323. The metric evaluation shows that, MSE is greater than zero which makes the datasets valid and reliable and higher RMSE score exemplifies that the larger errors are weighted in this research with lesser MAE score value. Thus it could be interpreted that the samples are reliable in the developed model with similarities in estimated and actual outcomes, where RMSE is a good fit with large error value based performance metric evaluation method.

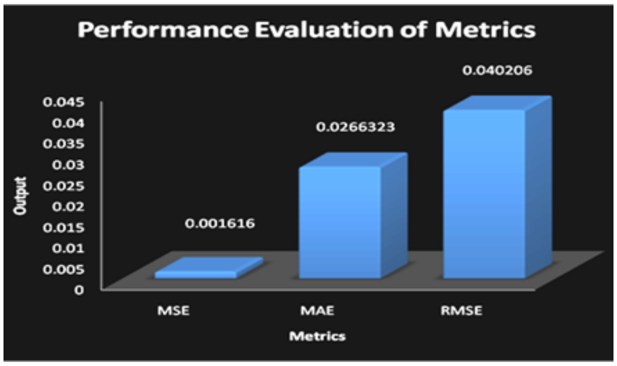


Figure 11 Performance Metrics

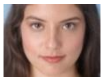
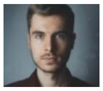
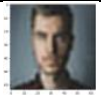
S. No	Input Image for Encryption	Encoded Image	First Encryption	Second Encryption	First Decryption	Second Decryption	Output Image after Decryption
1		[0.47021487,..., 1.0252512]	b'gAAAAABf... InH0Q=='	b'xf9-\xb5\xb9\... 19bQ\x905\'	'gAAAAABf... InH0Q=='	b'0.47021487... 1.0252512'	
2		[0.6836065,..., 0.19720754]	b'gAAAAABf... jEr0o=='	b'\xb1\x80\... xc7L\x86'	'gAAAAABf... jEr0o=='	b'0.6836065... 0.19720754'	
3		[0.9783868,... ,0.5129816]	b'gAAAAABf... Trd9=='	b'x9e\x8ae... \x80\xabUt'	'gAAAAABf... Trd9=='	b'0.9783868... 0.5129816'	
4		[0.5246873,... ,0.30762422]	b'gAAAAABf... Gwo78=='	b'\x8ae\x96\...x14\xf36'	'gAAAAABf... Gwo78=='	b'0.5246873... 0.30762422'	
5		[1.338901,..., 0.6813347]	b'gAAAAABf... Heu9e=='	b'\xb5\xc9>\... 05\x07'	'gAAAAABf... Heu9e=='	b'1.338901.. .0.6813347'	
6		[0.6196134,..., 0.54620165]	b'gAAAAABf... FInj8=='	b'\xb5\xc9... xdf\xf8kI\'	'gAAAAABf... FInj8=='	b'0.6196134... 0.54620165'	
7		[0.57934564,..., 0.08652248]	b'gAAAAABf... Isfd=='	b'<\xe1\xdc\... 573\x92'	'gAAAAABf... Isfd=='	b'0.57934564... 0.08652248'	
8		[1.2384509,..., 0.42446753]	b'gAAAAABf... Dds4o=='	b'\xde\xe0\...\x12Y\xbdj)\'	'gAAAAABf... Dds4o=='	b'1.2384509... 0.42446753'	
9		[0.5625143,..., 1.0581495]	b'gAAAAABf... fsa9Ad=='	b'6\xfc\xf5\x1... 2\x10('	'gAAAAABf... fsa9Ad=='	b'0.5625143... 1.0581495'	
10		[0.49479982,..., 1.338901]	b'gAAAAABf... Tef98=='	b'x0eS\xdf\x... \x83\xbd\'	'gAAAAABf... Tef98=='	b'0.49479982... 1.338901'	

Table 1: Outcome Obtained Through the Developed Model

7. CONCLUSION

Cloud computing, though considered as the great storage space for people to access and store their personal information, there are huge risks like, safety issues, privacy issues, security issues, data thefts, data piracy, data manipulation and mishandling, etc. However there are private security providers who indulge in developing algorithms ad safety measures and provide services for the users at feasible cost. The public cloud servers where the people are non-restricted towards accessing huge datasets and information are very prone towards higher risks and data loss. Henceforth researchers have been aiming to develop a secured ways of accessing and storing data in the private and public clouds where the users can retain personal and official information with certain alterations in the way of accessing and storing, known as encoding (encrypting) and decoding (decrypting) information through sender and the information receiver or the user.

The developed study aimed at data security and safety especially the "face images" in the cloud computing as inputs. The datasets were acquired from the UTK Face databank where numerous datasets with different variations, age, gender, and ethnicity have been focused. The developed model primarily focuses on pre-processing the original images and them passing them to double-level encryption where the Fernet and AES algorithms as hybrid model are utilized. Through these two-level encryption method the image will be passed through CNN and trained initially then once the encryptions (Fernet and AES) are a success, the images are stored and accessed through decryption where the (AES and Fernet) algorithms are applied and the vector image is processed and regenerated as original image (bitmap) and the face image as output is obtained through secure way.

The Sigmoid and ReLU activation functions along with MSE loss has been adopted as the statistical methods in this study and the obtained MSE, RMSE and MAE scores projects that the developed model is reliable and accurate towards securing and safeguarding information in cloud computing. The face as images is encoded and decrypted by the user efficiently where the data loss at training level and validation level is reduced to zero thus justifying that the model is efficient.

7.1. Scope for Further Research:

The current approach has been tested for only image datasets that are stored in the cloud. Other data that could be stored in cloud could be tested using the proposed approach. The model could be adopted and altered with different hybrid algorithms by future researchers for similar researchers and thus the research contributes information and base for upcoming future researchers. The scope for the research is higher since it is uses the hybrid model of AES and Fernet as algorithm for encrypting and decrypting. The adoption of these two algorithms is highly reliable where Fernet have become a complex symmetric encryption technique that technique that provides high encryption with Pseudo-polynomial method and AES provides standard security for high end users and large datasets.

REFERENCES

[1] D. Purushothaman and S. Abburu, "An Approach for Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, 2012, 9(2.1), pp. 100-105.

[2] P.B. Godhankar and D. Gupta "Review of Cloud Storage Security and Cloud Computing Challenges", (IJCSIT) International Journal of Computer Science and Information Technologies, 2014, 5(1), pp. 528-533.

[3] J. Puranik and A. Giri, "Security in Data Storage in Cloud Computing", International Research Journal of Engineering and Technology (IRJET), 2016, 3(6), pp. 1899-1902.

[4] N. Vurukonda and B.T. Rao, "A Study on Data Storage Security Issues in Cloud Computing", In 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016), Procedia Computer Science, 2016, 92, pp. 128-135.

[5] R. Wang, "Research on data security technology based on cloud storage", In 13th Global Congress on Manufacturing and Management, GCMM 2016, Procedia Engineering 2017, 174, pp. 1340-1355.

[6] A. Srivastava. (), "A survey report on Different Techniques of Image Encryption", International Journal of Emerging Technology and Advanced Engineering, 2012, 2(6), pp. 163-167.

[7] R. Kaur and K. Singh, "Image Encryption Techniques: A Selected Review", IOSR Journal of Computer Engineering (IOSR-JCE), 2013, 9(6), pp. 80-83.

[8] M. Kumar, A. Aggarwal and A. Garg, "A Review on Various Digital Image Encryption Techniques and Security Criteria", International Journal of Computer Applications, 2014, 96(13), pp. 19-26.

[9] H. Pan, Y. Lei and C. Jian, "Research on digital image encryption algorithm based on double logistic chaotic map", EURASIP - Journal on Image and Video Processing, 2018, (142), pp. 1-10.

[10] K. Mishra, R. Saharan. and B. Rathor , "A New Cryptographic Method for Image Encryption", Journal of Intelligent and Fuzzy Systems, 2017, pp. 1-9.

[11] N.M. Almutairy, and K.H.A. Al-Shqeerat, "A Survey On Security Challenges Of Virtualization Technology In Cloud Computing", International Journal of Computer Science & Information Technology (IJCSIT), 2019, vol. 11(3), pp. 95-105.

[12] A. Ghani, A. Badshah, S. Jan. et al., "Issues and challenges in Cloud Storage Architecture: A Survey", Researchpedia Journal of Computing, 2020, 1(1.6), pp. 50-65.

[13] N.R. Tadapaneni, "Cloud Computing Security Challenges", International Journal Of Innovations In Engineering Research And Technology [IJIERT], 2020, 7(6), pp. 1-5.

[14] A. Aliyu, A.H. Abdullah, O. Kaiwartya, et al., "Mobile Cloud Computing: Taxonomy and Challenges – A Review Article", Hindawi-Journal of Computer Networks and Communications, 2020,, pp. 1-23.

[15] J. Mahalakshmi and K. Kuppusamy. "An efficient Image Encryption Method based on Improved Cipher Block Chaining in Cloud Computing as a Security Service", Australian Journal of Basic and Applied Sciences, 2016, 10(2s), pp. 297-306.

[16] M. Sankari, and P. Ranjana, "Privacy-Preserving Lightweight Image Encryption in Mobile Cloud", In N. R. Shetty et al. (eds.), Emerging Research in Computing, Information, Communication and Applications, Advances in Intelligent Systems and Computing 2019, (882), pp. 404-415.

[17] S. Ayyub, and P. Kaushik, "Secure Searchable Image Encryption in Cloud Using Hyper Chaos", The International Arab Journal of Information Technology, 2019, 16(2), pp. 251-259.

[18] P.V. Lahande and P.R. Kaveri, “Increasing Data Secrecy In Cloud By Implementing Image Cryptography”, International Journal Of Scientific & Technology Research, 2020, 9(4), pp. 26-31.

[19] A. Altowaijri, M. Ayari and Y.E. Touati. “A Novel Image Encryption Approach for Cloud Computing Applications”, (IJACSA) International Journal of Advanced Computer Science and Applications, 2018, 9(12), pp. 440-445.

[20] K. Handa. and U. Singh., “Data Security in Cloud Computing using Encryption and Steganography”, International Journal of Computer Science and Mobile Computing, 2015, 4(5), pp. 786-791.

[21] I.N. Ibraheem, S.M. Hassan and S.A. Abead, “Comparative Analysis & Implementation Of Image Encryption & Decryption For Mobile Cloud Security”, International Journal of Advanced Science and Technology, 2020, 29(3s), pp. 109-121.

[22] I.A. Awan, M. Shiraz, M.U. Hashmi, et al., “Secure Framework Enhancing AES Algorithm in Cloud Computing”, Hindawi-Journal of Security and Communications Networks,2020, pp. 1-16.

[23] V. Bornare, K. Nikam, D. Khedkar and S. Hole, “Data Sharing with Sensitive Information Hiding for Secure Cloud Storage”, IJSRD - International Journal for Scientific Research & Development, 2020, 8(3), pp. 139-141.

[24] P.K. Chandaliya, V. Kumar, M. Harjani, et al., “SCDAE: Ethnicity and Gender Alteration on CLF and UTKFace Dataset”, Computer Vision and Image Processing, Springer Eds-Singapore, 2020, pp. 294-306.

[25] D. Datta, D. Mittal, N.P. Mathew and J. Sairabanu., “Comparison of performance of parallel computation of CPU cores on CNN model”, In Proc. 2020 Int. Conf. on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, Piscataway: IEEE, 2020, pp. 1-8.

[26] K. Nantomah. “On Some Properties of the Sigmoid Function”, Asia Mathematika, 2019, 3(1),pp. 79-90.

[27] A.F.M. Agarap, “Deep Learning using Rectified Linear Units (ReLU)”, 2019, Retrieved on 26th February 2021 from https://arxiv.org/pdf/1803.08375.pdf.

Authors

Ms Pronika is research scholar and assistant professor in Department of Computer Science & Engineering in Manav Rachna International Institute of Research and Studies. She has more than 13 years of experience in the field of research and teaching. She completed her B.tech from Kurukshetra University, Kurukshetra in 2007 and M.Tech from Banasthali Vidyapith, Jaipur in 2009. She has guided students in the field of cloud computing, network security, database and operating system. Currently, she is pursuing Ph.D from Manav Rachna International Institute of Research and Studies in the area of cloud computing. She has more than 25 publications in national / international journals and conferences in the field of computer science.

Dr. S. S. Tyagi is presently working as a Professor, Computer Engineering and Dean at Manav Rachna International Institute of Research and Studies (MRIIRS), Faridabad. He completed his B.Tech from Nagpur University, M.Tech from BITS Pilani and Ph.D from Kurukshetra University, Kurukshetra. He has more than 28 years of experience in the field of research and teaching. He is a senior member of many professional organizations like ACM, ASQ, IEEE, CSI, QCI etc. He has guided 06 Ph.D. and several M.Tech Thesis. He has more than 75 publication in national / international journals and conferences. His area of interest are cloud computing, Wireless Security, Computer Network, Ad hoc Networks etc.

How to cite this article:

Pronika, S.S.Tyagi, “Enhancing Security of Cloud Data through Encryption with AES and Fernet Algorithm through Convolutional-Neural-Networks (CNN)”, International Journal of Computer Networks and Applications (IJCNA), 8(4), PP: 288-299, 2021, DOI: 10.22247/ijcna/2021/209697.