ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 8, Issue 7, July 2021

Design and Development of Biometric System for Financial Document Verification Using Blockchain

[1] Saketh S Meka, [2] Rishan Rai, [3] Neeta B Malvi

[1][2 Student, ECE, RV College of Engineering, Banaglore, India
[3] Assistant Professor, ECE, RV College of Engineering, Banaglore, India

***Abstract*---Blockchain is an expanding list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data.To counter these problems of traditional databases, blockchain technology can be used instead. Blockchain technology is a decentralised storage network, where each data of each user/ customer is stored in blocks within their host systems, but the difference here is that, each block is connected with each other over the decentralized network using the hash values. Credential Verification is performed to check if the customer is original. Usual applications of customer profiling are done in the bank and security sector, where every new customer or user must undergo a background validation before his/her data is stored on the database. In usual practice, all the data collected by the banks are stored in a single, centrally controlled database. There are numerous disadvantages of the current system of storage of data. It is easy for the hackers to break through the database security and get all the customer's all details. Once the hacker or any unauthorized user accesses any one rows of the database, that person can access the entire database of sensitive information.**

In order to tackle this problem, one solution is to use decentralized blockchain technology replacing the old centrally owned database system. In this technology, every user's data will be stored in the blockchain. How blockchain works is that each block contains some data and using a cryptographic technique called secured hash algorithm 256 (sha256), the hash value of length 256 bits is calculated for every block. This hash value of a particular block is stored inside the next block, creating the blockchain. The use of blockchain here provides immense security as if the data of the block is accessed without authorization, and if the data is changed, the entire hash value for the block will be changed, and when this happens that particular block will get disconnected from the chain, and hence give an error signal. The blocks are stored in a server, but no human intervention can actually access these blocks, but only smart contract code blocks can access the blocks. Once the data is stored on the blockchain, it cannot be modified without authorization from the user. To use blockchain with authentication, facial recognition and audio recognition are used as security measures. The facial recognition model was trained using SVM and KNN for comparison purpose. KNN approach gave an accuracy of 96 % whereas the SVM approach gave an accuracy of 98%. The threshold for distance calculation was 0.58, at which it gave the maximum accuracy. Also the blockchain creation was done using python and hash for every block was calculated using SHA-256. Audio recognition was performed using Multi-Layer Perceptron model. An accuracy of 88 percent was achieved.

***Keywords*--- Blockchain, Python, Machine Learning, Neural Network**

I. INTRODUCTION

Blockchain is an expanding list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data. In order to counter these problems of traditional databases, blockchain technology can be used instead. Blockchain technology is a de-centralised storage network, where each data of each user/ customer is stored in blocks within their host systems, but the difference here is that, each block is connected with each other over the decentralized network using the hash values. Blockchain allows for a more precise method of storing data than traditional databases.

Procedure for Paper Submission

Paste Special | Picture (with "Float over text" unchecked).

The authors of the accepted manuscripts will be given a copyright form and the form should accompany your final submission.

II. METHODOLOGY

I A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. There are multiple methods in which facial recognition systems work, but in general, they work by comparing selected facial features from given image with faces within a database. It is also described as a Biometric Artificial Intelligence based application that can uniquely identify a person by analysing patterns based on the person's facial textures and shape [6].

While initially a form of computer application, it has seen wider uses in recent times on mobile platforms and in other forms of technology, such as robotics. It is typically used as access control in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems. Although the accuracy of facial recognition system as a biometric technology is lower than iris recognition and fingerprint recognition, it is widely adopted due to its contactless and non-invasive process . Recently, it has also become popular as a commercial identification and marketing tool. Other applications include advanced human-computer interaction, video surveillance, automatic indexing of images, and video database, among others

Holistic approach of facial recognition : In this approach, the complete face is consider as a single feature for detection and recognition. It compares the similarities of whole face, ignoring individual features like eyes, mouth, nose etc . These schemes are characterized into two parts:

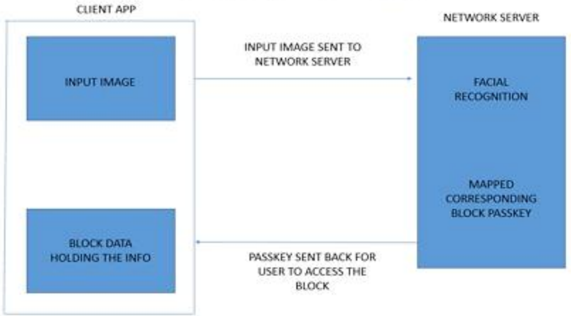
Statistical Approach: The face image density is calculated and the density set values are compared with the density values of databse images.This calculation is very expensive and directly suffering under the usual gaps pathways, such as face orientation scaling and illuminations. Artificial Intelligence Approach: Artificial Intelligence approach with tools such as neural networks and automatically recognizes the faces of learning techniques

Support vector machine: typical machine learning algorithm tries to find a boundary that divides the data in such a way that the misclassification error can be minimized. There can be several boundaries that correctly divide the data points. The two dashed lines as well as one solid line classify the data correctly.SVM differs from the other classification algorithms in the way that it chooses the decision boundary that maximizes the distance from the nearest data points of all the classes. An SVM doesn't merely find a decision boundary; it finds the most optimal decision boundary.

The most optimal decision boundary is the one which has maximum margin from the nearest points of all the classes. The nearest points from the decision boundary that maximize the distance between the decision boundary and the points are called support vectors. The decision boundary in case of support vector machines is called the maximum margin classifier, or the maximum margin hyper plane.

Audio Recognition- Audio is one of the most reliable methods of biometric security. The unique nature of each audio coupled with image recognition can increase the level of security of user data during financial transactions. The introduction of neural networks makes it possible to discern the minute differences in audio.The network learns by examining individual records, generating a prediction for each record, and making adjustments to the weights whenever it makes an incorrect prediction. This process is repeated many times, and the network continues to improve its predictions until one or more of the stopping criteria have been met. Initially, all weights are random, and the answers that come out of the net are probably nonsensical. The network learns through training. Examples for which the output is known are repeatedly presented to the network, and the answers it gives are compared to the known outcomes. Information from this comparison is passed back through the network, gradually changing the weights. As training progresses, the network becomes increasingly accurate in replicating the known outcomes. Once trained, the network can be applied to future cases where the outcome is unknown. Various models were used for this purpose details on working of each follows.

Audio Recognition using Multi Layer Perceptron Model : Multi-layer perceptron’s (MLP) are classed as a type of Deep Neural Network as they are composed of more than one layer of perceptrons and use non-linear activation which distinguish them from linear perceptrons. Their architecture consists of an input layer, an output layer that ultimately make a prediction about the input, and in-between the two layers there is an arbitrary number of hidden layers. These hidden layers have no direct connection with the outside world and perform the model computations. The network is fed a labelled dataset (this being a form of supervised learning) of input-output pairs and is then trained to learn a correlation between those inputs and outputs. The training process involves adjusting the weights and biases within the perceptrons in the hidden layers in order to minimize the error. The algorithm for training an MLP is known as Back propagation. Starting with all weights in the network being randomly assigned, the inputs do a forward pass through the network and the decision of the output layer is measured against the ground truth of the labels you want to predict. Then the weights and biases are back-propagated back though the network where an optimization method, typically Stochastic Gradient descent is used to adjust the weights so they will move one step closer to the error minimum on the next pass. The training phase will keep on performing this cycle on the network until it the error can go no lower which is known as convergence. The software we are implementing here is to create a blockchain network, where each user stores the user data on the blocks securely and if the user gives authentication to the block of data using facial recognition, only then can he/she access their own block with information. The blockchain data structure is a back-linked list of blocks of transactions, which is ordered. It can be stored as a flat file or in a simple database. Each block is identifiable by a hash, generated using the SHA256 cryptographic hash algorithm on the header of the block. Figure 3.1 depicts the approach used for the customer profiling system. The software to be implemented here is to create a blockchain network, where each user stores the user data on the blocks securely and if the user gives authentication to the block of data using facial recognition, only then can he/she access their own block with information. This is shown in the Figure 1.


CLIENT APP
NETWORK SERVER
INPUT IMAGE
INPUT IMAGE SENT TO NETWORK SERVER
FACIAL RECOGNITION
MAPPED CORRESPONDING BLOCK PASSKEY
BLOCK DATA HOLDING THE INFO
PASSKEY SENT BACK FOR USER TO ACCESS THE BLOCK

/Figure 1 /Customer social profiling and digital identity storage on blockchain approach diagram

The approach implemented here is to have each block of data created and stored on the client PC itself. However the passkey to open or access the block of data is present on the network.server. The network server doesn't hold the actual data, but holds the data and hash values of every block present in the chain. It also holds the information about which block is connected to which block with the help of hash codes, using a linked list data-structure. When a user wants to access his/her block of data, he or she uses his own face's picture and sends it to the network server. The network server performs facial recognition and identifies the unique hash associated with the particular user.

This unique hash is mapped to the unique passkey to open his/ her data block. The unique passkey is another random generated hash stored during the time of creation of the block of data.

The unique passkey is sent back to the client and the data block is opened to display the contents within it.

There are different steps involved in creation of the customer profiling system. First step is to create the blockchain with user data and the second step is to map the image embedding to the blocks.We create a data structure which holds the user name, id, bank account details etc. A block is build out of this which is a json object. This json object is used to create a unique hash using SHA256 algorithm. This algorithm is used to create a unique hash value of 256 hexadecimal values. The entire block can be accessed using this hash value. In extend to this, each block will hold the hash value of the previous block. This way the blockchain is created.The data entered by the user (name, age, gender etc) is first verified. The software program asks for an image of the aadhar card of the user. OCR is used and operated on the aadhar card and all the text is extracted from the image of the aadhar card. Also verhoeff algorithm is used to verify of the aadhar number is valid. On the extracted text, we use Natural language processing to extract and find the name, gender and dob. These values are then stored in a json file. The json file of the entered data and json file of aadhar data are compared.

Accessing the blockchain and getting data using biometric-For example, if we using facial recognition as biometric, the user's facial features are extracted and converted to a hash value. This hash value is maps to the SHA256 hash generated value for the user's block and gets the required data.

- Using the mapping of names to blocks, we can extract the information stored in the block of that user in the block chain.
- If the user wants to change any information about him in a particular block, then the user can do so by using his/her biometrics to access the block and changing it. But this would also change the hash value of that block.
- Hence all the hash values of all the blocks should be recalculated and assigned to the next block.

Audio Classification-

Data Collection for training: To train any neural network, it is necessary to have a viable set of training data. The training data that includes thousand sound signals of individuals saying the words 1-10 are used for neural network that can judges the polarity of the the sound signals.

To pre-process the data:For pre-processing process we shall be able to utilize Librosa load function. We will contrast the outputs from Librosa against the default outputs of scipy wavfile libraries by using a chosen file from the dataset. Librosa-load func5on will used to convert data the sampling rate to 22.08 KHz which we can utilize as our comparison levels.

Librosa's load func5on was used for bit rate in order to normalize the data so values range from -1 and 1 hence removing the complications of the dataset having a wider range of bit depth.We will extract Mel-Frequency Cepstral Coefficients (MFCC) extracted from the the audio samples. The MFCC represents the frequency distribution of the window sizes so it is permissible to analyse the frequency and 5me characteristics of the sound signals. The audio representations will permit us to characterize features for the classification process.

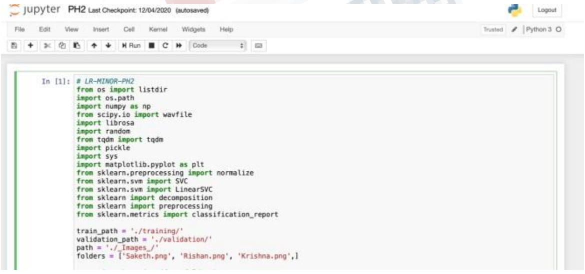
To make the neural network model: The formed vectors were then used to train a neural network. A stochastic gradient descent algorithm was found to best suit the requirement of minimum accuracy. A singular model was not found to be perfect. Then dual model of unigram and bigram processes was used which is basically dual level neural network.The objective to increase the modularity of the whole project, by making a low overhead architecture through varying the number of neurons and layers. The implementation was performed using python where the data was trained and validated using Logistic Regression, Support Vector Machine and Multi Layer Perceptron architectures with Soft-max activation. A variety of metrics are considered for evaluation: Accuracy, F1-Score, Precision Accuracy. The data was then combed using Multi Layer Perceptron model to reproduce requested sound signal from the raw data. Accuracy is one metric for evaluating classification models.

III. EXECUTION AND RESULTS

Blockchain is a data structure which holds the user data like name, date of birth, gender, aadhaar number etc. Apart from these variable details, it also holds the timestamp oh when the block was created and the hash of the previous block

For the initial block or the first block, the hash value is assigned to zero. The corresponding hash value for the initial or first block is calculated using SHA256 algorithm and stored in at temp file, which will be used by the next block, when created.The hash code for each block should be unique. If two blocks have exactly the same data present in them, then the hash code generated for those two blocks will also be same. Hence we use timestamp within the block which is unique for every block created, hence gives a unique 256 hexa-decimal hash code. he smart contract code is written which does the verification of the aadhaar number using verhoeff algorithm.

Next the blocks are created. If it is the first block in the chain, then hash code =0, else the previous hash code is written into the block.



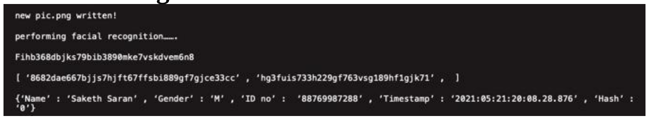
```
In [1]: # LR-MINOR-PH2
        from os import listdir
        import os.path
        import numpy as np
        from scipy.io import wavfile
        import librosa
        import random
        from tqdm import tqdm
        import pickle
        import sys
        import matplotlib.pyplot as plt
        from sklearn.preprocessing import normalize
        from sklearn.svm import SVC
        from sklearn.svm import LinearSVC
        from sklearn import decomposition
        from sklearn import preprocessing
        from sklearn.metrics import classification_report

        train_path = './training/'
        validation_path = './validation/'
        path = './_Images_/'
        folders = ['Saketh.png', 'Rishan.png', 'Krishna.png',]
```

/figure 2/ Training Metrics

Results- Facial recognition : The training metrics can be seen in the Figure . The figure shows a graph of different threshold on the X-axis and the distance metrics value (accuracy) accuracy on the Y-axis. The best suited threshold is 0.58, which gives the highest accuracy and calculates the closest match or the least distance between the pictures. The bar graph gives the negative matches and the positive match accuracies, for the particular threshold values. The best threshold value is found out by comparing accuracy for the all the threshold values from 0 to 1, in the steps of 0.2

/figure 3 / Credential verification



```
new pic.png written!

performing facial recognition……

Fihb368dbjks79bib3890mke7vskdvem6n8

[ ‘8682dae667bjjs7hjft67ffsbi889gf7gjce33cc’ , ‘hg3fuis733h229gf763vsg189hf1gjk71’ ,  ]

{‘Name’ : ‘Saketh Saran’ , ‘Gender’ : ‘M’ , ‘ID no’ :  ‘88769987288’ , ‘Timestamp’ : ‘2021:05:21:20:08.28.876’ , ‘Hash’ :
‘0’}
```

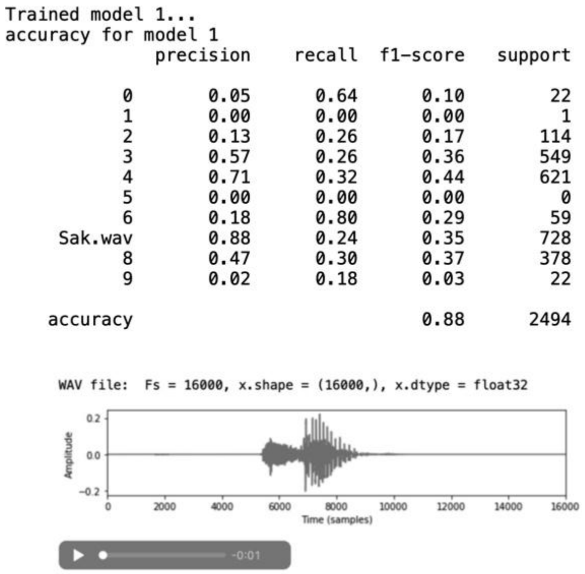
Implementation of Audio recognition: The implementation was performed using python where the data was trained and validated using Multi Layer Perceptron architectures with Softmax activation. A variety of metrics are considered for evaluation: Accuracy, F1- Score, Precision Accuracy. The data was then combed using Multi Layer Perceptron model to reproduce requested sound signal from the raw data.

Accuracy is one metric for evaluating classification models. Informally, accuracy is the fraction of predictions the model got right. Equation below defines the accuracy

AUC (ROC) Score: The Receiver Operating Characteristic (ROC) Curve is a very useful tool when predicting the probability of a binary outcome. It is a plot of the false positive rate (xaxis) versus the true positive rate (y-axis) for a number of different candidate threshold values between 0.0 and 1.0. **The True Positive Rate (TPR)** is calculated as the number of true positives divided by the sum of the number of true positives and the number of false negatives. It describes how good the model is at predicting the positive class when the actual outcome is positive. Equation below defines the true positive rate.

The False Positive Rate (FPR) is calculated as the number of false positives divided by the sum of the number of false positives and the number of true negatives. It is also called the false alarm rate as it summarizes how often a positive class is predicted when the actual outcome is negative. Equation below defines the false positive rate.

The Area Under the Curve (AUC): Score can be used as a summary of the model skill. Generally, skillful models are represented by curves that bow up to the top left of the plot Using machine learning algorithms, a simple speaker dependent speech recognition system is implemented that can recognize the spoken digits(1 to 10). Many other methods have been used effectively for voice recognition, such as paCern recognition methods, HMM methods etc. but here the Multi-layer Perceptron(MLP),. A speech recognition system, using the paCern recognition capabilities of supervised machine learning classifier, and other mathematical and signal processing tools will be able to correctly identify simple words. The system will recognize samples that it trained with, and will also be able to generalize to other samples of the same word. As larger vocabularies are used, recognition accuracy will decrease. The performance and accuracy of three different types of machine learning algorithms are compared.



```
Trained model 1...
accuracy for model 1
              precision    recall  f1-score   support

           0       0.05      0.64      0.10        22
           1       0.00      0.00      0.00         1
           2       0.13      0.26      0.17       114
           3       0.57      0.26      0.36       549
           4       0.71      0.32      0.44       621
           5       0.00      0.00      0.00         0
           6       0.18      0.80      0.29        59
     Sak.wav       0.88      0.24      0.35       728
           8       0.47      0.30      0.37       378
           9       0.02      0.18      0.03        22

    accuracy                           0.88      2494

    WAV file:  Fs = 16000, x.shape = (16000,), x.dtype = float32
```

/figure 4 / Results of MLP Audio Classifier

IV. CONCLUSION

The Blockchain is the new type of the database which solved some of the problems in the centralized system, such as the transactions without a middleman, the spent time on each transaction, the unintentional or special deletion or modification of data in the Blockchain. With the advantages of the technology, such as the transparency, trusty, the multiple copying of the transactions and the decentralized digital ledger, the Blockchain technology is reliable and not destructible, and all mentioned attacks could disrupt the system work, not the technology.Audio Classification was done using Multilayer perceptron method. An accuracy of 88 percent was achieved.The facial recognition model was trained using KNN approach and SVM. The SVM provides an accuracy of 98% and KNN approach provided 96% accuracy.

REFERENCES

[1] Chaturvedi, K. and Vishwakarma, D.K., 2020, January. Face Recognition in an Unconstrained Environment using ConvNet. In Proceedings of the 2020 2nd International Conference on Big Data Engineering and Technology (pp. 67-71).

[2] R. Rivera, J. G. Robledo, V. M. Larios and J. M. Avalos, ”How digital identity on blockchain can contribute in a smart city environment,” International Smart Cities Conference (ISC2), Wuxi, pp. 1-4, 2019.

[3] Kuperberg, Michael. ”Blockchain-based identity management: A survey from the enterprise and ecosystem perspective.” IEEE Transactions on Engineering Management 67.4 (2019): 1008-1027.

[4] Q. Stokkink and J. Pouwelse, ”Deployment of a Blockchain-Based Self-Sovereign Identity,” 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, pp. 1336-1342, 2018.

[5] Aradhana, Dr. S. M. Ghosh, “Secure Hash and Its Variants”, second International Conference on Contemporary Computing and Informatics, 2016.

[6] Hirotaka Yoshida, Alex Biryukov, “Analysis of SHA-256 variant”, National Institute of Advanced Industrial Science and technology conference August 2015. [7] A. R. S. Siswanto, A. S. Nugroho and M. Galinium, ”Implementation of face recognition algorithm for biometrics based time attendance system,” 2014 International Conference on ICT for Smart Society (ICISS), Bandung, pp. 149-154, 2014.

[8] J. K. Khan and D. Upadhyay, ”Security issues in face recognition,” 2017 5th International Conference - Confluence the Next Generation Information Technology Summit (Confluence), Noida, pp. 719-725, 2017.

[9] Neena Aloysius, Geetha M, “A Review on Deep Convolutional Neural Networks”, IEEE International Conference on Communication and Signal Processing (ICCSP), pp. 588 – 592, 2019.

[10] D. H. Hubel and T. N. Wiesel, “Receptive fields and functional architecture of monkey striate cortex”, The Journal of physiology, pp. 215 – 243, 2017.

[11] A. Songara, L. Chouhan, “Blockchain: A Decentralized Technique for Securing Internet of Things”. Conference paper, October 2017.

[12] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala and S. Elkhediri, ”CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques,” 2019 2nd International Conference on Computer Applications Information Security (ICCAIS), Riyadh, Saudi Arabia, pp. 1-6, 2019.

[13] Maria Rona L. Perez, Dr. Bobby Gerardo, “Modified SHA256 for Securing Online Transactions based on Blockchain Mechanism”, Technological Institute of the Philippines Aurora Blvd, 2018.

[14] Peters, Panayi, "Understanding modern banking ledgers through Blockchain Technologies: Future of transaction processing and smart contracts on the internet of money", University College London, 2018.

[15] D. Augot, H. Chabanne, O. Cl´emot and W. George, "Transforming Face-to-Face Identity Proofing into Anonymous Digital Identity Using the Bitcoin Blockchain," 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, pp. 25-2509, 2019.

[16] Sachchidanand Singh, Nirmala Singh, "Blockchain: Future of Financial and Cyber Security ", 2nd International Conference on Contemporary Computing and Informatics, 2017.