International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

A Robust Hybrid Biometric Face Recognition Payment System

Yashasvi Mutteneni, Shirisha Kasireddy, Anurag Achanta

Abstract: ***Modern civilization has always been endeavoring to achieve a cashless and digital society. The emergence of payment methods like cards, net banking, and digital wallets have enabled the possibility of cashless and cardless online and offline payments. However, these payment methods are at the risk of theft and sometimes may require users to memorize different passwords. Biometric Payments may seem like a viable option but, the fingerprints can be spoofed and dirt particles may damage the fragile sensors. Face recognition payments are more frictionless than the present card, mobile and biometric payment systems as they do not require a device to carry out the transaction. It is also reliable, secure and efficient. Hence, saving time for both the customer and retailer. The previous system used Eigenfaces and Euclidean Distance for face recognition payment. Our proposed system uses Haar Cascades for face detection and Local Binary Patterns Histogram(LBPH) for face recognition. Our proposed approach is more efficient with respect to parameters such as noise reduction, threshold, training time, confidence and accuracy as it achieves a higher noise reduction and accuracy with a lower threshold, training time and confidence.***

Keywords: Cardless Payment, Face Detection, Face Recognition, Haar Cascades, Local Binary Pattern Histogram, OpenCV.

I. INTRODUCTION

Now-a-days, data privacy is a major concern in today's technology driven and fast paced world making security more important than ever before. Consequently, Reliable security systems are crucial for not only preventing but also limiting the losses due to identity theft. This has stimulated researchers to innovate new solutions for the improvisation of security systems, especially those involving human identity. The conventional methods of payment cannot be relied on as they can be forged, manipulated and even stolen. In addition, traditional security methods like keys and cards can be lost or misplaced. Thus a simple and efficient payment system has to be developed to overcome these drawbacks. Biometric methods can be implemented as they present a higher degree of security when compared to traditional methods [10].

Manuscript received on March 15, 2020.
Revised Manuscript received on March 24, 2020.
Manuscript published on March 30, 2020.

Yashasvi Mutteneni*, Department of Computer Science and Engineering, JNT University, Hyderabad, India. Email:yashincontrol@gmail.com

Shirisha Kasireddy, Department of Computer Science and Engineering, JNT University, Hyderabad, India. Email:shirishakasireddy20@gmail.com

Anurag Achanta, Department of Computer Science and Engineering, JNT University, Hyderabad, India. Email:anuragachanta19@gmail.com

As the human face is unique, it offers much higher security and efficiency than other techniques [7]. Systems that are capable of detecting and recognizing faces can be applied to a wide range of applications including payments, criminal identification and surveillance systems [9].Face detection and recognition involves convoluted and rigid algorithms making it a tedious task [5]. The main difference between the two is that face detection deals with identifying the presence of a face in an image or video and, face recognition works by taking an image of a face and making a prediction of whether the face matches with another face in the database[1]. On the one hand, recognizing a face is a natural process and humans tend to do it effortlessly. On the other hand, application of this process in the field of computer vision still tends to be a convoluted problem.

In the present work we have used enhanced approaches for secure online and offline payments using face identity. Literature survey is illustrated in Section II, Methodology is proposed in section III, Results in section IV, conclusion in section V, and Future scope in section VI.

II. LITERATURE SURVEY

Today, biometric payment is being widely used by countries all over the world. Fingerprint payment which is based on finger scanning is the most widely used biometric payment method. The system generally uses a two factor authentication in which the finger scanner is used in place of the card swipe and then the user enters in the PIN as usual. In this way, Fingerprint scanning is used as a cardless and cashless payment method [11]. This technology recognizes individuals based on a few distinctive physical attributes which can be difficult, if not impossible to copy or forge, thus making it much more secure than traditional security methods like PIN numbers, signatures, social security numbers and passwords. The benefits provided by the biometric finger scanner are evident as they offer very high accuracy and are one of the most economical biometric authentication techniques present today [8]. In addition, they are easier, faster and cheaper to set up. Therefore, fingerprint payment offers faster checkout and makes transactions safer for the customers. However, this biometric technology is not error free as it often faces difficulty in scanning and authentication in unhygienic conditions and could thus lead to false rejections. Repositioning fingers is time consuming. Furthermore, the real problem of fingerprint payments is the extent of damage resulting from a stolen identity. Stolen cards and secret PIN numbers can be replaced with new cards and new PIN numbers, but stolen fingerprints cannot be replaced with new prints [2].

The above biometric technology requires unique hardware and software making it considerably expensive. Security of the account and personal details are at risk due to false acceptance and false rejection. To overcome these drawbacks, an efficient face recognition system was developed using Eigenfaces and Euclidean Distance Vector[7]. Facial recognition offers an automatic, quick and seamless verification experience. It also offers seamless integration as no specific hardware is required. A simple mobile or webcam is enough. Both Eigenfaces and Fisherfaces consider dominant features of the training set as a whole. Speed of recognition is increased by storing unknown pattern vectors in the pattern space [12]. However, since the eigenfaces method is scale sensitive, it requires some preprocessing for scale normalization. In addition, recognition rate decreases under varying pose and illumination. Finally, using eigenfaces and fisher faces for face recognition is not an elegant solution since confidence and threshold is high, background noise is maximum, and efficiency is low [6].

Since all the above technologies and algorithms lack in noise reduction and security and accuracy enhancement, we have designed a face recognition payment system using LBPH.

III. METHODOLOGY

In this paper, we have proposed a trustworthy immune payment system with face recognition. To understand our approach the process has been explained in a chronological order (algorithm) below.

ALGORITHM:

- Capturing of Dynamic or Static Image.
- CVTColor(): to convert from BGR to Grayscale.
- Apply Haar Cascade for face detection and extraction with integrated techniques as
  - "Haar features" extraction
  - Integral Images
  - AdaBoost: to improve classifier accuracy
  - Cascade of classifiers
- Divide face image into blocks.
- Calculate histogram for each block.
- Combining 'LBPH' histograms into a single histogram.
- Face image is processed.
- Recognition Result.
- Payments

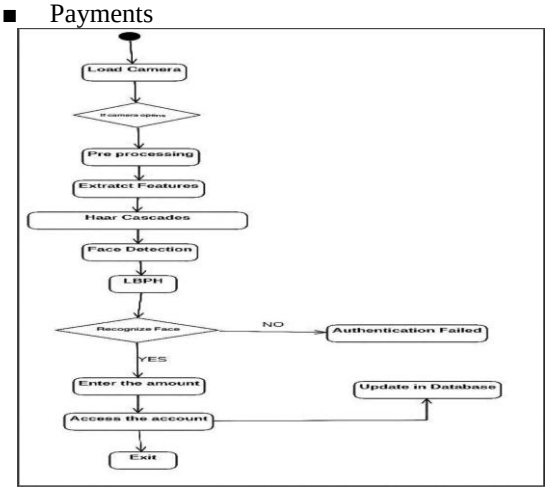

Fig. 1: Complete flowchart of our approach.

A. Conversion of RGB to Grayscale:

From cvtColor, we have used the function to convert BGR to Grayscale. Transformations such as elimination or addition of the alpha channel is to be carried out within the RGB space. BGR color to grayscale conversion is done using [3]:

RGB[A] to Gray:Y←0.299· R+0.587· G+0.114· B

gray=cv2.cvtColor(img,cv2.COLOR_BGR2GRAY);

B. Haar Cascades:

The Haar cascades algorithm works as described below.

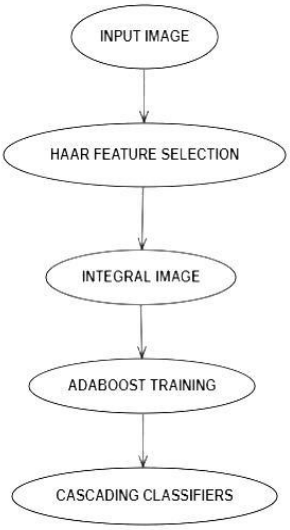

Fig. 2: Haar Cascades algorithm

a. 'Haar Features' extraction:

Haar features or Haar-like features are those used to classify generic objects. These are the prime features for face detection using which the system classifies whether an image is a face or not. The image is segmented by shrinking down the region of interest. Basically, haar features are like windows which are placed upon images to calculate a single feature. The feature is a single value that is obtained by the subtraction of pixels under the white and black regions[3]. This information is stored in a file known as haar-cascade which is generally an XML format file. A noticeable amount of work is required to train the classifier system as well as generate the cascade file. This can be visualized in the diagram below:

Fig. 3: Haar-like features

b. Integral Images:

An Integral image lets you analyze aggregates of image subregions swiftly. These aggregates are useful in many applications, like analyzing HAAR wavelets. These are generally applied in face recognition and other alike algorithms.

Suppose an image is *x* pixels wide and *y* pixels high. Then the integral of this image will be *x+1* pixels wide and *y+1* pixels high. The first column and row of the integral image are all zeros. Any other pixel shall have the sum of all the pixels before them as the value assigned to them[3].

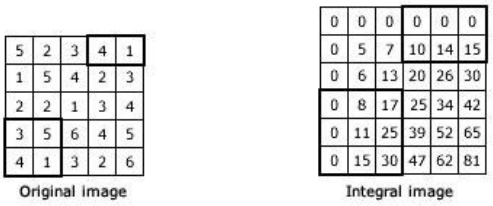

Fig. 4: Original and Integral Images

Now, for approximation of the pixel aggregate in the black box, the respective box in the integral needs to be taken. You can find the sum as follows: (Bottom right + top left - top right - bottom left). So for the box with 3,5,4,1, the analysis would go like this: (30+0-17-0 = 13). For the box with 4,1, it would be (0+15-10-0 = 5).

In this way, the aggregate in rectangular regions can be analyzed swiftly.

c. Adaboost:

In Adaptive Boosting a.k.a. AdaBoost, over 180,000 features result in a 24X24 window. However, not all features are useful to identify a face. To select the unique features out of all the available ones, a machine learning algorithm called Adaboost is adapted. The core concept used here is the identification of the best features essential for recognizing a face. It is performed by the construction of a strong classifier which is a linearly combined group of weak classifiers. As a result, a drastic decline of features from 180,000 to 6000 is observed.

d. Cascade of Classifiers:

Cascade of classifiers helps the haar cascade algorithm perform fast. The cascade classifier consists of several stages where each stage consists of a strong classifier. This is helpful to eliminate the need of applying all the features on the window at once. Instead, it groups the features into different sub-windows and at each stage, the classifier decides whether the sub-window is a face or not. If a face is not detected, the sub-window and it's features are discarded. However, if a face is identified, the sub-window moves past the classifier and then carries onto the next stage where the second round of features are applied. The entire process can be understood more clearly in the diagram below[3].

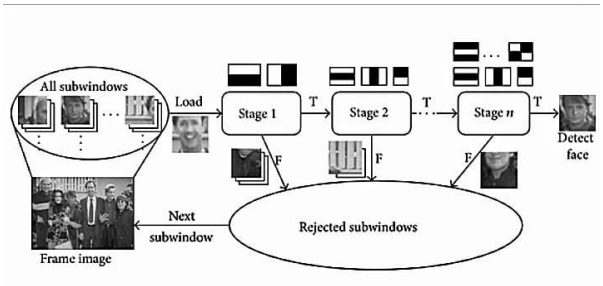

Fig. 5: Cascade of classifiers process

C. Local Binary Patterns Histogram:

Extracting features from input test image and then matching them with the faces in the system's database is the key feature of LBPH.

The steps involved to achieve this are:

- Creating dataset
- Face acquisition
- Face extraction
- Classification

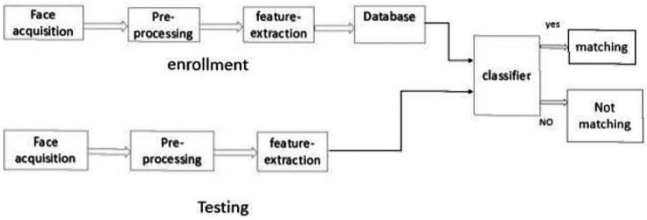

Fig. 6: The flowchart of LBPH algorithm.

Let us consider an image with dimensions L x B. We now chip the image into square blocks where it results in B x B dimension for every region[3].

Fig 7: Image processing in LBPH

The local Binary operator is defined in a window of 3x3 and is used for every region.
A formal description of the LBP operator is given as:

$$LBP(x_c, y_c) = \sum_{p=0}^{P-1} 2^p s(i_p - i_c)$$

Where (x_c, y_c) is the central pixel with intensity i_c; and i_n is the intensity of the neighbor pixel. Here S is given as:

$$s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

Using the median pixel value as threshold, the pixel is compared to its 8 closest pixels using the above function. If the value of the neighbor lies starting from the central value to any greater value, it is set as 1, else it is set as 0. Hence, we have obtained a total of 8 binary values from the 8 neighbors. After these values are combined, an 8 bit binary number is obtained which is then translated to a decimal number for our convenience. This decimal number is known as the pixel LBG value and has a range of 0-255[4].

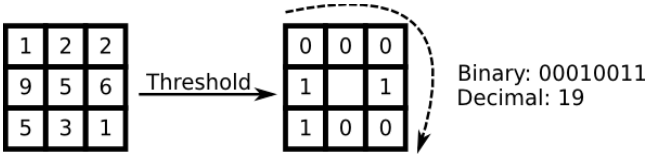

Fig. 8:Extraction of LBP feature from the image

Later it was found that a fixed neighborhood fails to encode details varying in scale. So the algorithm was improved to use a different number of radius and neighbors.

This algorithm is now known as circular LBP.

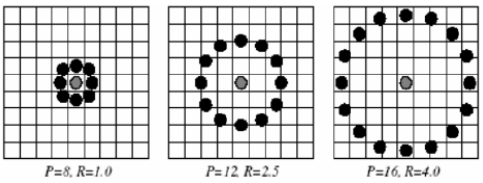

Fig. 9: Circular LBP

The main idea in this algorithm is to align a random number of neighbors on a circle with variable radius. Neighborhoods are captured in the following way:

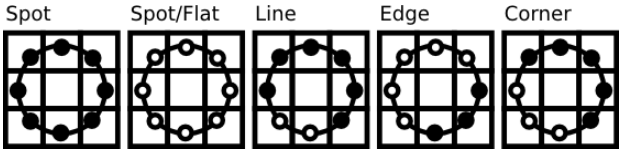

Fig. 10: Representation of variable neighborhoods

For any given Point (x_c, y_c), the position of the neighbor $(x_p, y_p), p \in P$ can be calculated by:

$$x_p = x_c + R\cos\left(\frac{2\pi p}{P}\right)$$

$$y_p = y_c - R\sin\left(\frac{2\pi p}{P}\right)$$

Here, R is the radius of the circle whereas P is the number of sample points. If the points coordinate on the circle does not correspond to image coordinates, it gets generally interpolated by bilateral interpolation

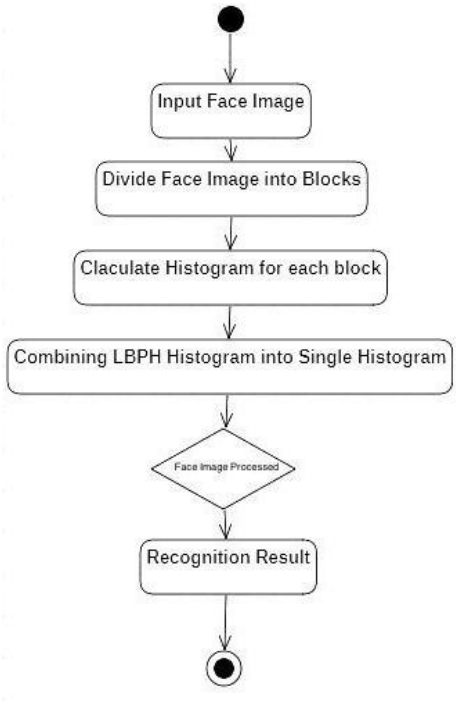

Fig. 11: LBPH Algorithm

The LBP operator is potent against monotonic gray scale transformations [4]. After the LBP value is generated, the histogram of the region is then created by counting the number of similar LBP values in the region. When histograms are generated for each region, all of them are merged to become a mono histogram. This is the feature vector of the image. Finally, the histograms of the test image and images in the database are compared and the image with the closest histogram is returned.We get the ID of the image from the database if the image is recognized:

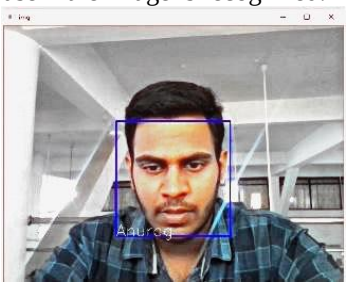

Fig. 12: Face Recognition

D. Accessing Account and making payment:

Once the camera is loaded, the test image is compared with the trained images in the database. If a match is found, the user's name will be displayed and the user's account will be accessed.

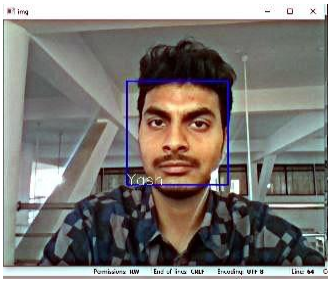

Fig. 13: Identification before account access.

The payment system activates where the user receives a prompt indicating to enter the money to be paid.

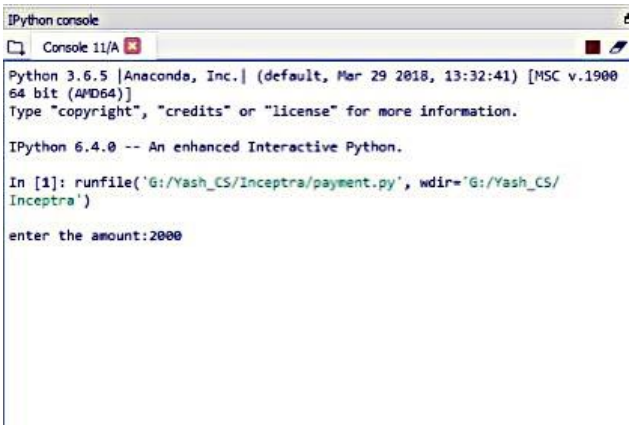

Fig 14: Amount entry after account access.

After the amount is entered the following conditions are checked:

- If the amount entered by the user is more than the account balance, the transaction will be unsuccessful and a message will be stated to the user saying that he does not have sufficient balance.
- If the amount entered by the user is less than the account balance, then the transaction will be successfully carried out and the money will be deducted from the user's account automatically as shown below:

```
mysql> use bank
Database changed
mysql> select* from payment;
+-------+---------+----------------+-----------+--------------+
| regid | regname | initial_amount | deducted  | final_amount |
+-------+---------+----------------+-----------+--------------+
|     1 | Yash    |          10000 |      2000 |         8000 |
|     2 | Anurag  |          50000 |     15000 |        35000 |
+-------+---------+----------------+-----------+--------------+
2 rows in set (0.23 sec)
```

Fig. 15: Updated bank database after successful transaction

IV. RESULTS

TABLE-I: Comparison of different algorithms

CRITERIA	EIGEN FACE+Distance Classifier	FISHER FACE+distance Classifier	Haar Cascade classifier +LBPH
Noise	Maximum	Medium	Minimum
Threshold	4000	400	7
Training time	Highest	Medium	Least
Confidence	2,000-3,000	100-400	2-5
Accuracy	Least	Higher than Eigen Face	Highest

Compared to pre-existing approaches our approach proved to be better in many parameters such as training time, confidence , threshold, noise and accuracy.

V. CONCLUSION:

This paper presents the viability of payments through face recognition using the most efficient face recognition algorithm in OpenCV. In the present work, the biometric face recognition based payment system is used for both online and offline cardless transactions. It is found to be more safe, user friendly and secure. The image is analysed independently and works in different environments and light conditions. If an unauthorized person tries to access the account by showing their face, the buffer value will be more than 2.2e+04 and the account access will be forbidden. Haar Cascade and LBPH outperforms other algorithms with confidence factor in range 2-5 and Threshold at 7.5. The false positive rate is found to be 22% along with high efficiency and minimum noise interference. In existing systems, the combination of LBPH and Distance Classifier has a training time of 0.5 sec, whereas our approach with the combination of LBPH and Haar Cascade classifier proves to be better a training time of 0.3 sec.

VI. FUTURE SCOPE

In the proposed Face Recognition Payment System, we used Local Binary Patterns Histogram for recognizing faces. The ability of face recognition system can be further improved by using LBPH for feature extraction along with Convolutional Neural Networks(CNN) for classification of the images as the correspondence between the trained images helps CNN to converge faster and achieve a better accuracy. Furthermore, Human Gait and Human Posture recognition can be used for enhanced security.

ACKNOWLEDGMENT

First and Foremost, We would like to express our sincere gratitude towards our advisor Assoc. Prof. Shirisha Reddy for her continuous support towards our research, for her inevitable love, patience, motivation, enthusiasm, and immense knowledge. Her guidance helped us throughout the research and writing of this research paper. We could not have imagined having a better advisor and mentor for our research.

Besides our advisor, We would like to thank Dr. Gopa Dutta,(Prof.& Director.R&D) and the Research and Development center of VBIT , for their encouragement, insightful comments, thoughtful questions, and provision of appropriate requirements.

REFERENCES

1. https://www.datacamp.com/community/tutorials/face-detection-python-opencv
2. https://www.ifsecglobal.com/cyber-security/4-drawbacks-of-biometric-authentication/
3. https://www.docs.opencv.org/2.4/modules/contrib/doc/facerec/facerec_tutorial.html
4. V. B. T. Shoba and I. S. Sam, "Face Recognition Using LBPH Descriptor and Convolution Neural Network," 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2018, pp. 1439-1444.
5. Kaur, Jashanpreet & Akanksha, & Singh, Harjeet, "Face detection and Recognition: A review,"6th International Conference on Advancements in Engineering & Technology (ICAET-2018)
6. http://www.ijsrp.org/research-paper-0218/ijsrp-p7433.pdf
7. https://www.ijert.org/research/biometric-face-recognition-payment-system-IJERTCONV6IS13107.pdf
8. Nikita Bakshi and Vibha Prabhu, "Face recognition system for access control using principal component analysis," 2017 International Conference On Intelligent Communication And Computational Techniques(ICCT),Manipal University Jaipur, Dec 22-23,2017
9. Chinchu. S, Anisha Mohammed and Mahesh B S, "A Novel Method for Real Time Face Spoof Recognition for Single and Multi-User Authentication," 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT).
10. D. Kumar, Yeonseung Ryu and Dongseop Kwon, "A survey on biometric fingerprints: The cardless payment system," 2008 International Symposium on Biometrics and Security Technologies, Islamabad, 2008, pp. 1-6.
11. Dileepkumar and Yeonseungryu, "A Brief Introduction of Biometric and Fingerprint Payment Technology," 2008 Second International Conference on Future Generation Communications and Networking Symposia
12. M. A. Turk and A. P. Pentland, "Face recognition using eigenfaces," Proceedings. 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Maui, HI, USA, 1991, pp. 586-591.

AUTHORS PROFILE

Mrs. Shirisha Kasireddy is currently working as an Associate Professor in the Department of Computer Science and Engineering at VBIT, Hyderabad, India. She has a teaching experience of over 15 years. She is also an IEEE WIE coordinator. She has submitted her research work in the domain of security and integrity in Cloud Computing from JNT University, Hyderabad, India. She has obtained her M.Tech from the School of Information Technology, JNT University, Hyderabad and her B.Tech from JNT University, Hyderabad. Her research interests include cloud computing, cryptography and machine learning. She has published 8 research papers in national and international journals and has attended 2 Conferences.

Yashasvi Mutteneni is an undergraduate Computer Science and Engineering student at VBIT, JNT University, Hyderabad, India. His research interests include Artificial Intelligence, Machine learning, Computer Vision, Natural Language Processing and Deep Learning. He interned at Bharat Dynamics Limited, Hyderabad, India. He has built socialnet.hyd for the COVID-19 Global Hackathon, which is a website that helps small businesses regain their lost income. He has also done other projects such as Content Similarity Identification, Crop Yield Predictor ML Model and VBIT Marketplace. He has secured a global rank of 596 and country rank of 73 in the IEEEXtreme Programming Competition 13.0. He has also been ranked in the top 25% of all test takers in the Euclid Math contest, conducted by The Centre for Education in Mathematics and Computing, University of Waterloo, Canada.

Anurag Achanta is an undergraduate Computer Science and Engineering student at VBIT, JNT University, Hyderabad, India. His research interests include cryptography, IOT, machine learning, artificial intelligence and cyber defence and offence mechanisms. He had designed a Manet communication gadget that can be adapted in several fields of forces. He had developed a tool for penetrating any device running OS such as iOS, MacOs, Windows, Linux and Android. He has scored an Iq score of 148. He has been G-35345 ISO certified by ORBIT TECHNOLOGY RESEARCH PRIVATE LIMITED where he obtained 99%. He has been iIAS ISO certified as international administrator where he obtained 99%.. He is a personality development mentor for many of the undergraduates.