ZKG INTERNATIONAL ISSN: 2366-1313

ENHANCED SECURITY FEATURE FOR ATM'S THROUGH FACIAL RECOGNITION

[1]Mrs. G .Swathi, [2] R. Veda Sri, [3] P.Keerthi [4] V.Srija

[1]Assistant Professor, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad,

goguswathi@gmail.com

[2,3,4,]BTech Student, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad

vedasrirapolu2202@gmail.com, pusapatikeerthi@gmail.com, srijareddyvarakuti@gmail.com

ABSTRACT :

Automated Teller Machines also known as ATM's are widely used nowadays by each and everyone. The ATM machine (Automated Teller Machine) is an electronic device that is used by the banks to perform banking tasks like withdrawal of money, transferring of money, and many to get many information about a user's bank account without the need to visit a bank. This System revolutionized the way of transactions. There were no long lines of queue in front of the bank for a simple withdrawal of money. The number of ATM's a bank has can be a factor in considering the strength of a bank. As there is increase in the number of ATM's, there is also increase in the fraudulent activities in the ATM. The main motivation of this project is to increase the security feature of the use of ATM. The current method uses static key (PIN) for security. The proposed method uses Face-id as a key incorporated with current method. The advantages can be found as that the face-id is unique for everybody; it cannot be used by anybody other than the user. In this project we are using Histogram algorithm and Machine learning techniques are used to identify the personals using the machine. This system uses Open CV to process the image being obtained to detect the faces in the image. The face recognition is done using Local Binary Pattern Histogram Algorithm. Local Binary Pattern (LBP) is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number.

Keywords *:* - Long Short-Term Memory (LSTM), Deep learning, Machine learning .

ISSN: 2366-1313

I INTRODUCTION

In an increasingly connected and technological world, ATM security is a top priority for financial institutions and their customers. Security methods such as PIN and card verification have limitations. To solve these issues, we propose “Using Facial Recognition to Improve ATM Security.” Facial recognition using artificial intelligence and computer vision is revolutionizing data security and user access. This approach not only increases ATM security but also improves user experience. Thanks to unique facial recognition, ATMs provide an extra layer of protection against unauthorized access, card theft and fraud. Deep neural networks will be used to recognize faces and identify each person's unique face. In this article titled "Using facial recognition to increase ATM security", we will explore its content, benefits and advantages over traditional methods. Integration of advanced technologies such as facial recognition using deep neural networks (DNN) will be an important strategy to strengthen ATM security infrastructure.

Authentication is the process of verifying the identity of an individual or entity. In the view point of ATM card transactions, it ensures that the person using the card is indeed the legitimate owner .Without effective authentication, several issues can arise, including:

1. Fraudulent Transactions: Inadequate authentication opens the door to unauthorized access. Fraudsters can misuse stolen or lost cards, leading to financial losses for both customers and banks.

2. Lengthy Transaction Process: Manual verification methods, such as physical signatures, can be time consuming .Lengthy processes inconvenience customers and slow down transaction speeds.

3. Lack of Customer Confidence: Customers need assurance that their transactions are secure. Weak authentication erodes trust and may discourage card usage.

4. Higher Transaction Costs: Dealing with fraudulent transactions or resolving authentication-related disputes increases operational costs for financial institutions.

To address these challenges, various authentication methods are employed:

1. **Demographic Authentication**: This involves matching the demographic information like name, address etc., provided by the cardholder with the data stored in the central database .It’s a basic form of validation.

2. **One-Time PIN (OTP) Authentication**: A time-limited OTP is sent to the cardholder’s registered mobile

number .The user provides this OTP during the transaction, ensuring an additional layer of security.

3. **Biometric Based Authentication**: This data is used to find the cardholder identity .This method enhances security and convenience.

4. **Multifactor Authentication**: Combining 2 or more authentication modes that strengthens security.

II. LITERATURE SURVEY

1. Facepin: Face Biometric Authentication System for Atm Using Deep Learning.

Author: A Kowshika, P.Sumathi , K S Sandra, et al.Year: 2022

An automatic teller machine security model that would combine a physical access card and electronic facial recognition using Deep Convolutional Neural Network. If this technology becomes widely used, face recognition techniques used, and details would be protected as well as their accounts.

2) Cardless Transaction of ATM Machine with Asecurity of Facial Recognition and OTP with Shuffle Keypad.

Author: Dhamale Omkar, Auti Sahil et al. Year: 2022.

An ATM with this system authenticates users by looking at their faces. Every human has a different facial feature, making it possible to identify the individual specifically. The user must scan his face with the sensor before the system takes it and searches the database.

3. Face Recognition Based New Generation ATM Machine.

Author: B.Prasad, D. Sahithi, et al.Year: 2021.

The usage of nothing involves more than a PIN and access card to confirm uniqueness. By stealing cards, PINs, customer account information, and other security measures, ATMs that use face recognition systems show how easy it is to make false claims and treat people unfairly they use cardless transactions where misuse of a card or stolen card will not by user

4. Face Recognition Open CV Based ATM Security System.

Author: A.D. Gujar, N.B Sawant, T.L Hake, et al. Year: 2023.

The step of feature extraction involves identifying the distinctive elements of the camera image. Check out if all of your facial features are visible. This feature vector

ISSN: 2366-1313

effectively represents the face. in order to protect ATMs against theft and prevent ATM robberies. It takes the place of the ATM system used traditionally.

III SYSTEM ANALYSIS

EXISTING SYSTEM

A simple multi-factor authentication setup involves asking a stoner for their username and word(commodity they know) as well as vindicating their identity through a alternate factor similar as an SMS communication to their phone(commodity they have). That covers two factors of authentication, but adding in image recognition as well adds an redundant subcase of security to the login process without making it frustrating or exorbitantly complicated for authorized druggies.

Limitations of Existing system

1. Leg law verification is enough.
2. Scanning the glamorous strip in the ATM cards will give the complete details of the card.

PROPOSED SYSTEM

This design proposes an new subcase of security to compound the being ATM system pricing that deals calculate not only on the correct Leg entry of a card but also on the verification of stoner's identity. The methodology employed in this design revolves around the application of standard perpetration ways, specifically face recognition using the Original Binary Pattern Histogram algorithm, which has been enforced using OpenCV Python.

Proposed system Advantages:

- That proposed system proves to be effective in terms of securing deals and reducing the time needed for authorized druggies to complete deals.

IV IMPLEMENTATION

Architecture:

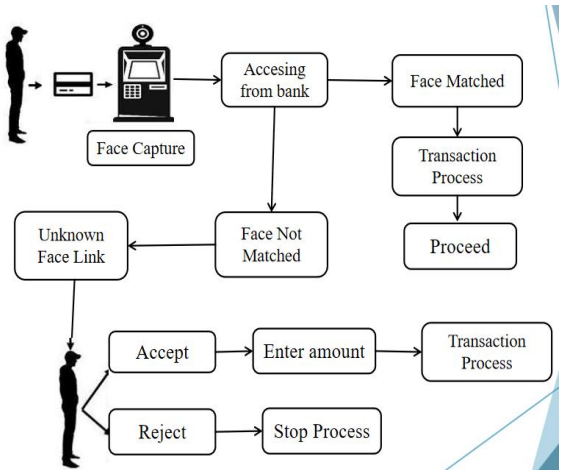


Fig-1. Architectures of the system model

Methodology

The human face is identified using the Histogram of Oriented Gradients (HOG) method. Affine transformation of the face is done using the dlib library. A Deep Convolutional Neural Network (Deep CNN) is trained to get unique measurements from the human face (128 different measurement from a single face), and Support Vector Machine (SVM) for face classification (identification).

Here we are using Local Binary Pattern (LBP) as our base face recognition algorithm. This algorithm is efficient and has been customized for our specific purpose and more efficient face recognition. It is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number.

We implement the LBPH using OpenCV. OpenCV was started at Intel in 1999 by **Gary Bradsky** and the first release came out in 2000. Right now, OpenCV supports a lot of algorithms related to Computer Vision and Machine Learning and it is expanding day-by-day.

Currently OpenCV supports a wide variety of programming languages like C++, Python, Java etc. and is available on different platforms including Windows, Linux, OS X, Android, iOS etc. Also, interfaces based on CUDA and OpenCL are also under active development for high-speed GPU operations. OpenCV-Python is the Python API of OpenCV. It combines the best qualities of OpenCV C++ API and Python language.

Python is a general purpose programming language started by Guido van Rossum, which became very popular in short time mainly because of its simplicity and code readability. It enables the programmer to express his ideas in fewer lines of code without reducing any readability.

- **LBPH: (Local Binary Pattern Histogram)**

Local Binary Pattern (LBP) is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighborhood of each pixel and considers the result as a binary number.

LBP is combined with histograms of oriented gradients (HOG) descriptor, it improves the detection performance considerably on some datasets.

Parameters: the LBPH uses 4 parameters:

- Radius:
- Neighbors

- Grid X
- Grid Y

Radius: the radius is used to build the circular local binary pattern and represents the radius around the central pixel. It is usually set to 1.

Neighbors: the number of sample points to build the circular local binary pattern. Keep in mind: the more sample points you include, the higher the computational cost. It is usually set to 8.

Grid X: the number of cells in the horizontal direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.

Grid Y: the number of cells in the vertical direction. The more cells, the finer the grid, the higher the dimensionality of the resulting feature vector. It is usually set to 8.

Training the Algorithm: First, we need to train the algorithm. To do so, we need to use a dataset with the facial images of the people we want to recognize. We need to also set an ID (it may be a number or the name of the person) for each image, so the algorithm will use this information to recognize an input image and give you an output. Images of the same person must have the same ID. With the training set already constructed, let's see the LBPH computational steps.

Applying the LBP operation: The first computational step of the LBPH is to create an intermediate image that describes the original image in a better way, by highlighting the facial characteristics. To do so, the algorithm uses a concept of a sliding window, based on the parameters **radius** and **neighbors**.

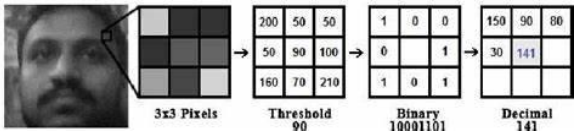


Fig- 2 : LBP operation

Extracting the Histograms: Now, using the image generated in the last step, we can use the **Grid X** and **Grid Y** parameters to divide the image into multiple grids

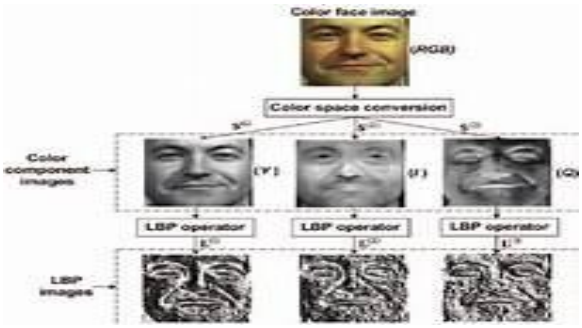


Fig- 3 : Extracting the histogram

- **OpenCV Python**

ISSN: 2366-1313

OpenCV-Python is the Python API of OpenCV. It combines the best qualities of OpenCV C++ API and Python language.

Python is a general purpose programming language started by Guido van Rossum, which became very popular in short time mainly because of its simplicity and code readability. It enables the programmer to express his ideas in fewer lines of code without reducing any readability.

Compared to other languages like C/C++, Python is slower. But another important feature of Python is that it can be easily extended with C/C++. This feature helps us to write computationally intensive codes in C/C++ and create a Python wrapper for it so that we can use these wrappers as Python modules. This gives us two advantages: first, our code is as fast as original C/C++ code (since it is the actual C++ code working in background) and second, it is very easy to code in Python. This is how OpenCV-Python works, it is a Python wrapper around original C++ implementation.

And the support of Numpy makes the task more easier. Numpy is a highly optimized library for numerical operations. It gives a MATLAB-style syntax. All the OpenCV array structures are converted to-and-from Numpy arrays. So whatever operations you can do in Numpy, you can combine it with OpenCV, which increases number of weapons in your arsenal. Besides that, several other libraries like Matplotlib which supports Numpy can be used with this. So OpenCV-Python is an appropriate tool for fast prototyping of computer vision problems.

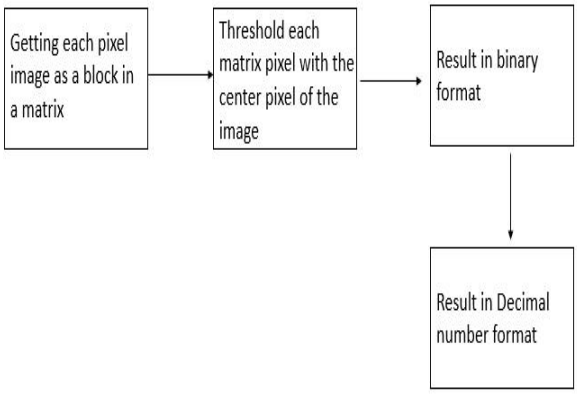
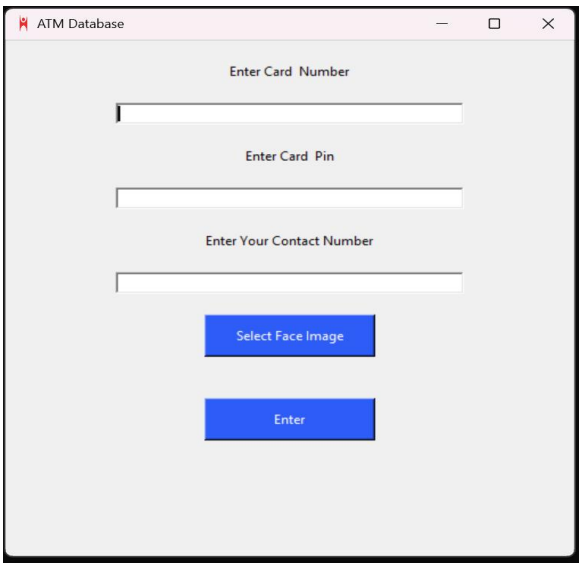


Fig- 4 : Block Diagram of Proposed

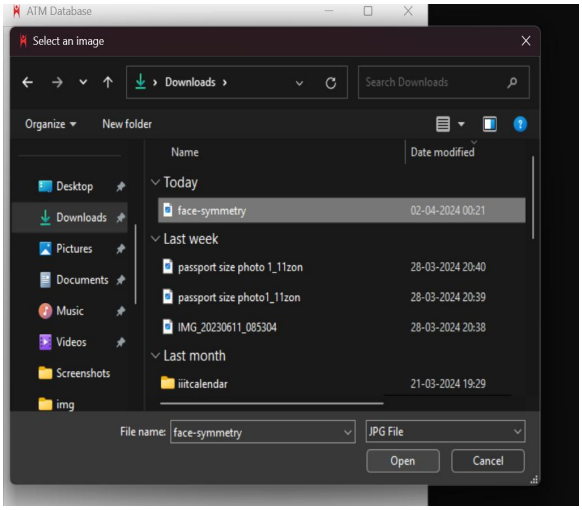
V RESULT AND DISCUSSION

Admin page:

ISSN: 2366-1313

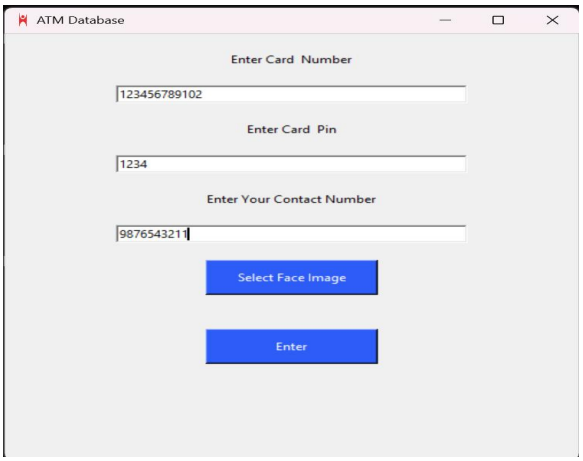


Select the image

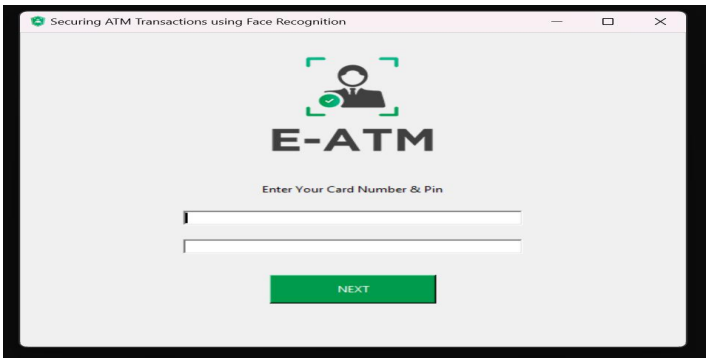


Insert the image

Enter details:

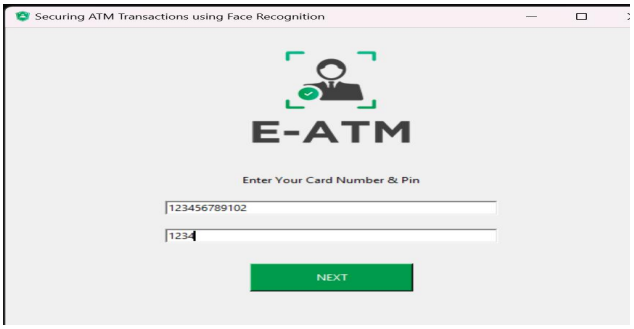


User page

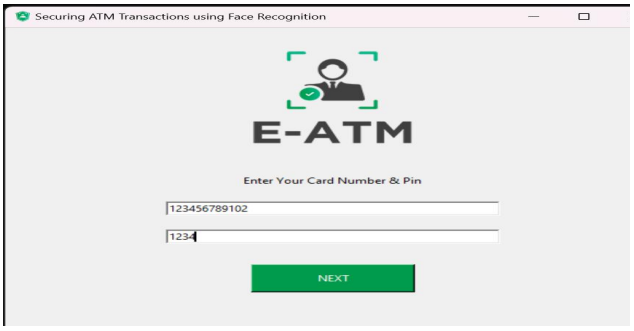


ISSN: 2366-1313

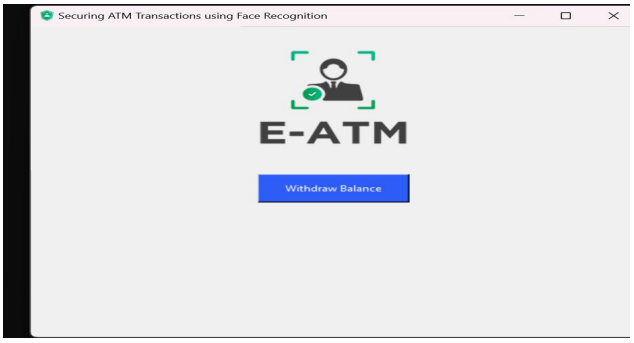
Login



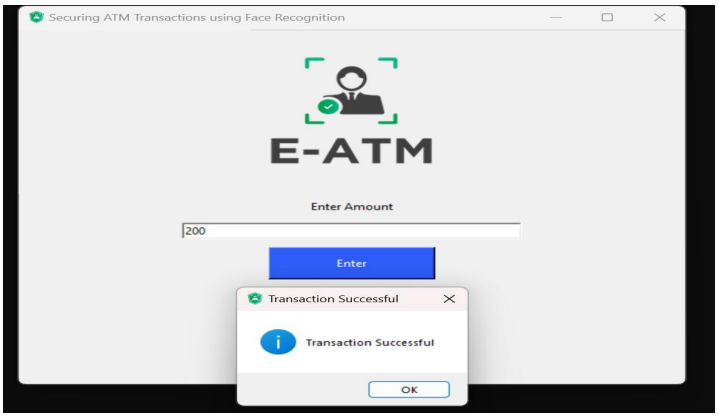
Proceed



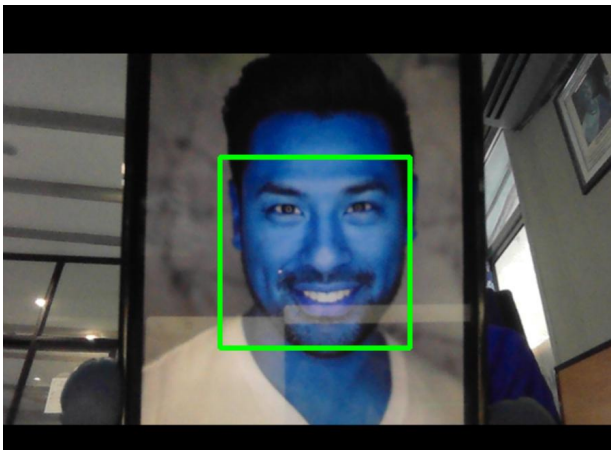
Shows withdraw balance



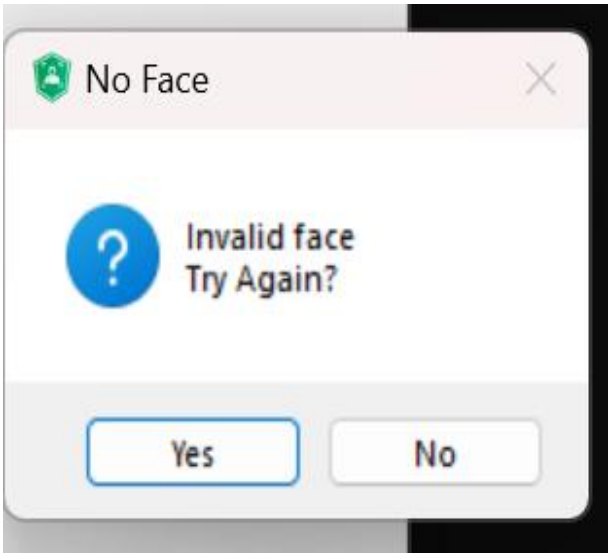
Enter amount and successful transaction



Compare the face



Rejected as invalid face



VI CONCLUSION

The method what we proposed is far better in increasing the security feature. The main goal of our paper is to incorporate the facial recognition feature along with the existing conventional method for the betterment of the user. The LBPH algorithm used here is used for the comparing the face of the user with the face in the database. Machine learning is used to train (used in OpenCV inbuilt face recognizer) the face recognizer. The main limitation of this system is that it requires periodic maintenance of the cameras. Twins can be an exception in this system. In rare cases, photos can be used to bypass the security. The future scopes of this method are that the use of high-quality durable cameras. 3-d cameras can be used for the condition of twins and photo bypassing.This project can overcome the issue of impersonation of a cardholder. This is like a two factor authentication method which is used to confirm that the transaction is done by the card owner or the persons trusted by the owner using face recognition. It limits the card usage of the unauthorized users who hold the password of someone's card. Thus, this ATM model provides security against exploitation of identity, by using a verification system using face recognition to the identity and confirm the user and it will scale back forced transactions to an excellent extent.

FUTURE ENHANCEMENT

A promising topic with tremendous potential in the future is the use of facial recognition technology to protect ATM transactions. Customers may be correctly and promptly recognized with this technology, reducing fraud and raising security.

Customers may access their accounts without using real ATM cards by integrating the technology with mobile apps. This provides more convenience while lowering the danger of card skimming and other forms of fraud. We may anticipate significant developments in facial recognition technology in the future, such as increased accuracy and quicker processing times. This will strengthen its ability to secure ATM transactions and safeguard users' financial Information.

VII REFERENCES

1. E.Derman, Y.K.Gecici and A.A.Salah, Short Term Face Recognition for Automatic Teller Machine (ATM) Users, in ICECCO 2013, Istanbul, Turkey, pp.111-114.https://dx.doi.org/10.21172/1.841.20

2. JinfangXu, Khan, Rasib and RasibHasan, SEPIA: Secure-PIN-authentication-as-a-service for ATM using Mobile and wearable devices, 3 rdIEEE International Conference on Mobile Cloud Computing, Services, and Engineering IEEE, June 2015,pp. 41-50.
3. Marilou O. Espina1, Arnel C. Fajardo, Bobby D. Gerardo, RujiP. Medina, Multiple Level Information Security Using Image Steganography and Authentication, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.6, November – December 2019, pp.3297-3303. https://doi.org/10.30534/ijatcse/2019/100862019
4. M.Murugesan, R.Elankeerthana, Support vector machine the most fruitful algorithm for prognosticating heart disorder , International, Journal of Engineering and Technology, Volume 7, pp.48 – 52, 2018. https://doi.org/10.14419/ijet.v7i2.26.12533
5. M.Murugesan,S.Thilagamani, Overview Of Techniques For Face Recognition, International Journal Of Life Science and Pharma Reviews , pp.66 - 71 , 2019 ,
6. ISSN 2250 – 0480. https://dx.doi.org/10.22376/ijpbs/10.SP01/Oct/2019
7. M.Murugesan, R.Elankeerthana, Pedestrian ReIdentification Using Deep Learning, International Journal Of Life Science and Pharma Reviews, pp.71 - 78 , 2019 , ISSN 2250 – 0480.
8. P.Pandiaraja, N. Deepa, A Novel Data PrivacyPreserving Protocol for Multi-data Users by using genetic algorithm, Journal Soft Computing Volume 23 Issue 18, pp8539-8553, 2019.
9. S.Karthikeyan, S.Sainath, K.P.TharunAswin, K.Abimanyu, An Automated Anti-Theft and Misusealerting System for ATM, IOSR Journal of Electronics and Communication Engineering (IOSRJECE), Volume 10, Issue 2, Ver. II (Mar - Apr.2015), PP 97-102.
10. P.RajeshKanna, P.Pandiaraja, An Efficient Sentiment Analysis Approach for Product Review using Turney Algorithm, Journal of Procedia, Computer Science ,Volume 165, Issue 2019, PP 356-362. https://doi.org/10.1016/j.procs.2020.01.038
11. Sri Vasu, Subash, Sharmila Rani, Udhayakumar,ATM Security using Machine Learning techniques in IOT,

International Journal of Advance Research, Ideas and
12. Innovations in Technology, Volume 5, Issue 2, pp. 150- 153, 2019.

AUTHORS

Mrs. G .Swathi, Assistant Professor Dept. of CSE, Teegala Krishna Reddy Engineering College Meerpet, Hyderabad.
Email: goguswathi@gmail.com
Miss. R.Veda Sri,Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.
Email: vedasrirapolu2202@gmail.com
Miss. P.Keerthi, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.
Email: pusapatikeerthi@gmail.com
Miss. V.Srija, Dept. of CSE, Teegala Krishna Reddy Engineering College, Meerpet, Hyderabad.
Email: srijareddyvarakuti@gmail.com