iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51803

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Advanced High Secured Smart ATM System

Narmatha R[1], Reshma J[2], Jeevitha K[3], Janani C[4]
[1, 2, 3]*UG Scholar,* [1]*Assistant Professor , Department of Computer Science and Engineering, Avinashilingam Institute for Home Science and Higher Education for Women School of Engineering, Coimbatore-641006.*

Abstract: Automated Teller Machines are widely used nowadays by people. But It's hard to carry their ATM card everywhere, people may forget to have their ATM card or forget their PIN number. The ATM card may get damaged and users can have a situation where they can't get access to their money. In our proposal, use of biometrics for authentication instead of PIN and ATM card is encouraged. Here, The Face ID is preferred to high priority, as the combination of these biometrics proved to be the best among the identification and verification techniques. The implementation of ATM machines comes with the issue of being accessed by illegitimate users with valid authentication code. This project provides service to the user only when the user is legitimate or the user is verified by the legitimate user of the ATM card. The users are verified by comparing the image taken in front of the ATM machine, to the images which are present in the database. If the user is legitimate the new image is used to train the model for further accuracy. This system uses openCV to process the image being obtained and Haar Cascade Classifier to detect the faces in the image. The face recognition is done using Local Binary Pattern.To overcome these problems,the project 'ATM Security system based on Face recognition, PIN and OTP' consists of conventional features ie is Personal Identification Number (PIN) along with additional features like face recognition and one-time password (OTP) is used. Database holds information about a user's account details, images of his/her face and a mobile number which will improve security to a large extent.

Keywords: ATM frauds prevention model, Smartphone for secure ATM transactions, ATM transaction security system, ATM attacks.

I.INTRODUCTION

A. Automated Teller Machine

An Automatic Teller Machine (ATM) is a computerized machine that is used to withdraw cash from a customer's respective bank account. As financial users prefer ATM for cash withdrawals, cash deposits and many other transaction, the banks are focusing a lot over the security of ATMs.Hence ATM should be protected properly from the criminal activities or from any unwanted things.

B. Artificial Intelligence In Atm Security

ATM is an automated teller machine which is a computerized telecommunication device that provides customers with access to financial transactions in public space without the need for a human clerk or bank teller. ATM machines integrated with Artificial intelligence with the use of biometric authentication such as fingerprint and face detection reduces the risk of frauds.With the use of two way authentication, associated with web application the security system is further enhanced and notified by the users when accessed without their knowledge. Thus Combinations of all these technologies may help in reducing the ATM frauds and hence can improve the security level of other financial transactions.

II.LITERATURE REVIEW

1) *A two-steps prevention model of ATM frauds communications. Ossama H. Embarak Dept. of Computer Sciences Higher Colleges of Technology Abu Dhabi, UAE.*

This paper proposes a two steps model to complete ATM transactions using a closed end-to-end fraud prevention system. By adding a smartphone as an additional layer for ATM transactions, and using legitimate user smartphone ID numbers to robust ATM secure transactions using the available technologies. The genuine client smartphone as an intermediate tool where financial institutions will maintain not only customer PIN number but also customer smartphone device ID (physical device identification), which is a unique number associated with a smartphone and is separate from hardware serial numbers. Bank base application (BBA) installed on the bank back-end system (BES), while the front-end application on ATM (AATM) is used as a medium between the end-user and BES, as well as on the genuine user smartphone (GSTP). When the genuine user starts his ATM transaction and enters a correct PIN number, the ATM system (AATM) should ask the user to select either barcode or transaction PIN number (TPN).

©IJRASET: All Rights are Reserved

A request should be sent to the bank system (BES) requesting to start an ATM transaction for the logged in user. Bank system has two options: either generate a barcode or transaction PIN number using hash function, each composite of random transaction number and the user 's smartphone device physical ID. Genuine user's smartphone device physical ID number registered in the bank system. Bank system should update its database records with the user transaction permission field, including the generated barcode or transaction PIN number as per user selection on the ATM. Bank system will reply to the ATM by sending a generated barcode or transaction PIN number. Accordingly, the Bank system implement the defined hash method using the installed application (GSTP) to generate barcode or TPN as per the defined hash function.The main aim of using user's smartphone device is that even if fraudster got legitimate user authentication PIN number, the fraudster would not be able to perform a transaction without users' registered smartphone physical device, not the CIM number. Furthermore, if a fraudster gains access to the user's smartphone device, he should not know the user's PIN number which should be used to begin a transaction. The only situation in which the fraudulent can complete the transaction is when he has the user's smartphone physical device, CIM card and user's PIN number which we expect is sporadic.

2) One Touch Multi-banking Transaction ATM System using Biometric and GSM Authentication:

One Touch Multi-banking Transaction ATM System using Biometric and the account details of all the bank accounts of account holders are displayed. User needs to select one of the bank accounts for the transaction. If the user wants to transfer the money or debit the money from the account he/she will get OTP on the registered mobile number. The GSM module generates OTP to enforce authenticate transactions from the bank side.

3) Enhanced Security for ATM Machine with OTP Authors:Mohsin Karovaliya

Mohsin Karovaliya in paper proposes an Eigenface based method for face recognition. The model shows the qualitative analysis of algorithms used based on the metrics of existing algorithms. According to the statistics, PCA based face recognition is very accurate, requires less computation time and less storage space as trainee images are stored in the form of their projections on a reduced basis. The drawback of using Eigenface based method is that it can sometimes be spoofed by the means of fake masks or photos of an account holder.

To overcome this problem 3D face recognition methods can be used. However, its computation cost is high.The paper suggests a vibration sensor which senses vibrations produced from ATM machines whenever robbery occurs. This system uses an ARM controller based embedded system to process real time data collected using the vibration sensor. Once the vibration is sensed the beep sound will occur from the buzzer.

DC Motor is used for closing the door of an ATM. Some other additional security measures are used. This will prevent the robbery and the person involved in the robbery can be easily caught. Software implementation is deployed using two software packages, first one is the Keil Vision 3.0. Second one is the Flash magic simulator. Keil Uvision Debugger accurately simulates on-chip peripherals. This system helps in rapid reaction and minimization of loss by detecting the ATM machine in real-time when it has been stolen can be found through GSM technology.

4) Enhanced security for ATM machine with OTP and Facial recognition features Saifali Karediab , Sharad Ozac , Dr.D.R.Kalbanded

The purpose of this paper is to reinforce security of the conventional ATM model. We have posited a new concept that enhances the overall experience, usability and convenience of the transaction at the ATM. Features like face recognition and One-Time Password (OTP) are used for the enhancement of security of accounts and privacy of users. Face recognition technology helps the machine to identify each and every user uniquely thus making face as a key. This completely eliminates the chances of fraud due to theft and duplicity of the ATM cards. Moreover, the randomly generated OTP frees the user from remembering PINs as it itself acts as a PIN.

Due to rapid development in science and technology, upcoming innovations are being built-up with strong security. But on the other hand, threats are also being posed to destroy this security level. Though enhancement in automation has made a positive impact overall, various financial institutions like banks and applications like ATMs are still subjected to thefts and frauds. The existing ATM model uses a card and a PIN which gives rise to an increase in attacks in the form of stolen cards, or due to statically assigned PINs, duplicity of cards and various other threats.

©IJRASET: All Rights are Reserved

III.EXISTING SYSTEM

A. *Eigenfaces Face Recognizer*

In this algorithm, a facial image is a point from a high-dimensional image space and a lower-dimensional representation is found, where classification becomes easy. The lower-dimensional subspace is found with Principal Component Analysis(PCA), which identifies the axes with maximum variance. While this kind of transformation is optimal from a reconstruction standpoint, it doesn't take any class labels into account.Imagine a situation where the variance is generated from external sources, let it be light. The axes with maximum variance do not necessarily contain any discriminative information at all, hence a classification becomes impossible.

B. *Limitations Of Eigen Face Algorithm*

To understand the difference between eigenfaces and Fisher faces. Basically, eigenfaces is PCA applied to face data and Fisher faces is LDA applied to face data. The eigenface recognition method bears some common disadvantages due to its appearance-based" nature. First, learning is very time-consuming, which makes it difficult to update the face database. Second, recognition is efficient only when the number of face classes is larger than the dimensions of the face space otherwise the projection of an unknown image requires pixel-by-pixel multiplication of the input image by all eigenfaces, which is equivalent to or worse than template-matching with respect to computation time since an extra distance calculation is needed in the subspace. However, the occurrence of class overlapping increases when more face classes are represented by the same face space, thus lowering the recognition rate.

IV.PROPOSED SYSTEM

A. *Fisher Face Algorithm*

Fisherface is one of the popular algorithms used in face recognition, and is widely believed to be superior to other techniques, such as eigenface because of the effort to maximize the separation between classes in the training process. Image recognition using fisherface method is based on the reduction of face space dimension using Principal Component Analysis (PCA) method, then apply Fisher's Linear Discriminant (FDL) method or also known as Linear Discriminant Analysis (LDA) method to obtain feature of image characteristic. The algorithm used in the process for image recognition is fisherfaces algorithm while for identification or matching face image using minimum euclidean.

V.BLOCK DIAGRAM

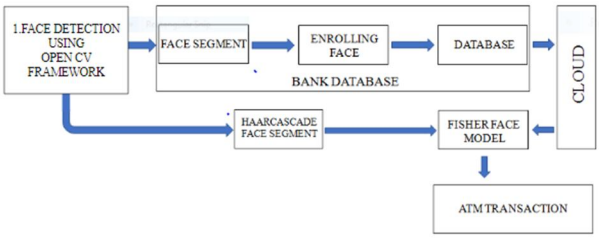


Fig 1 Transaction Using Face Detection

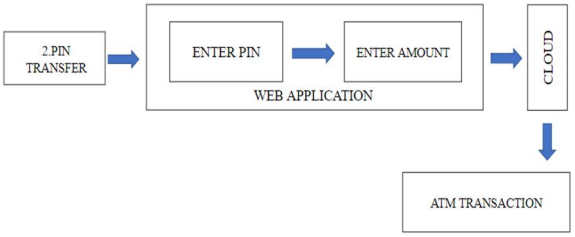


Fig 2 Transaction Using Web Application

VI.MODULE DESCRIPTION

1) Module 1: Face enrollment and creating database .

The user should first enroll their face with the bank and all the bank details of the user should be stored in the bank database.

2) Module 2: Training dataset using fisher face algorithm.

The system will be trained with the dataset using the fisher face algorithm.

3) Module 3: Developing GUI for atm interface

An atm interface is developed for image processing.

4) Module 4: Segmenting face using haar-cascade classifier

The haar-cascade classifier segments the captured image into positive and negative images and processes only the required image.

5) Module 5: Developing the application for third user

The web application is developed to send alert messages for two step verification and to use the pin transfer option.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

VII.IMAGE PROCESSING

The design of this process is divided into two stages:
Preprocessing stage and Processing stage which includes feature extraction and recognition.

1) *Preprocessing Stage:* Getting images using camera or saved images and conversion from RGB to grayscale. Image data is divided into training and test data.
2) *Processing Stage:* Fisherface method will be applied to generate the feature vector of facial image data used by the system and then to match the vector of traits of the training image with the vector characteristic of the test image using euclidean distance formula.

A. Feature Generation Process

Features to be extracted is a feature of the face image of people of Papua. The method used is fisherface method is a method that is a merger between PCA and LDA methods.

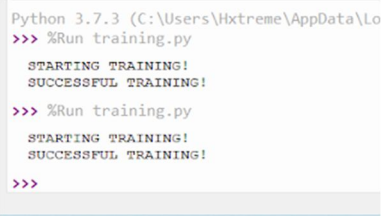


FIG 3 Training dataset using fisher face algorithm

VIII.SYSTEM DESIGN

A. The System Design

Face recognition system using fisherface method is designed to recognize the face image captured in the webcam by matching the results of its feature extraction with the images stored in the bank database.

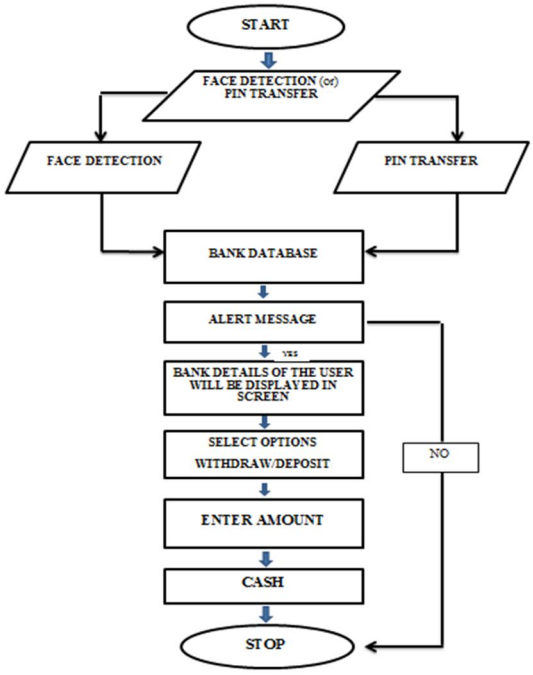


FIG 4 WORKING OF THE SYSTEM

Face detection is a technique that identifies or locates human faces in digital images.Face detection is performed by using classifiers. A classifier is essentially an algorithm that decides whether a given image is positive(face) or negative(not a face). A classifier needs to be trained on thousands of images with and without faces. Fortunately, OpenCV already has two pre-trained face detection classifiers, which can readily be used in a program.

©IJRASET: All Rights are Reserved

The two classifiers are:

1) Haar Classifier and

2) Local Binary Pattern(LBP) classifier.

In this article, however, we will only discuss the Haar Classifier.

Haar feature-based cascade classifiers

Haar-like features are digital image features used in object recognition. They owe their name to their intuitive similarity with Haar wavelets and were used in the first real-time face detector. Paul Viola and Michael Jones in their paper titled "Rapid Object Detection using a Boosted Cascade of Simple Features" used the idea of Haar-feature classifier based on the Haar wavelets. This classifier is widely used for tasks like face detection in computer vision industry.Haar cascade classifier employs a machine learning approach for visual object detection which is capable of processing images extremely rapidly and achieving high detection rates.These Haar Features are like windows and are placed upon images to compute a single feature. The feature is essentially a single value obtained by subtracting the sum of the pixels under the white region and that under the black.

Thus, when the feature window moves over the eyes, it will calculate a single value. This value will then be compared to some threshold and if it passes that it will conclude that there is an edge here or some positive feature.

IX.CONCLUSION AND FUTURE ENHANCEMENT

Facial recognition has proven to be one of the most secure methods of all biometric systems to a point for high level security and to avoid ATM robberies and provide security for ATM.In the proposed project, it replaces the traditional ATM system. It has advantages such as saves manufacturing cost of cards and overcomes drawbacks of the traditional system like carrying the ATM card, losing of card, fraud calls related to ATM card, etc.With new improved techniques in the field of artificial Intelligence that help eliminate more disturbances and distortions, the rate of effectiveness of the system can be improved

REFERENCES

[1] Jose Ferdinand; Cindy Wijaya; Andreas Noel Ronal; Ivan Sebastian Edbert; Derwin Suhartono " ATM Security System Modeling Using Face Recognition with FaceNet and Haar Cascade" 6th International Conference on Informatics and Computational Sciences (ICICoS) , 2022.

[2] Selvakumar R; Logesh S; Maha Vishnu S; Maniraj S; Praveen Kumar "A Face Biometric Authentication System for ATM using Deep Learning" 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), 2022.

[3] Prof. Anil. D. Gujar, Nikita B Sawant, Tejas L Hake, Aadesh A Shete, Shreekar M Deshmukh "Face Recognition Open CV Based ATM Security System"(IJRASET), 2022.

[4] Darwin Nesakumar A1 *, T Suresh2 , Nivedha T3 , K Nivedha S4 , Priyadharshini G5 , P Mugilan6 "Smart ATM Security Using Face Recognition ",European Journal of Molecular & Clinical Medicine", 2020.

[5] Pratiksha Shetiya,Meryl Mascarenhas,Mrunal Deshmukh ATM Security System using Iris Recognition by Image Processing "International Journal of Engineering Research & Technology", July 2020.

[6] D.ArunKumar; B. Iniyan; M. Ahamed Askar; A. Ajay; R. Ambika "Face Recognition Based New Generation ATM Machine" 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 2019.

[7] Manoj V , M. Sankar R , Sasipriya S , U. Devi E, Devika T , "Multi Authentication ATM Theft Prevention Using iBeacon", International Research Journal of Engineering and Technology (IRJET),2018.

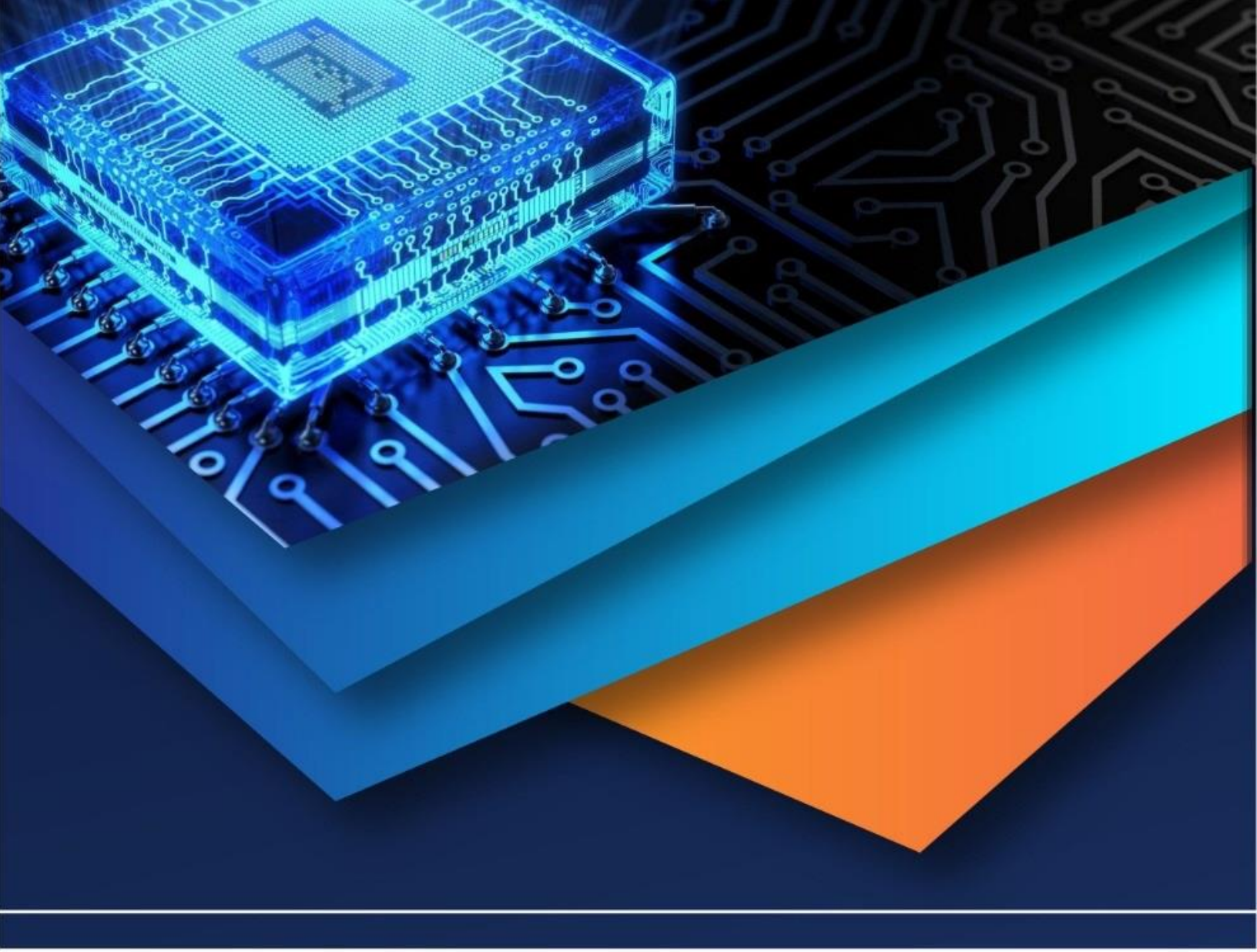
[8] Ossama H. Embarak, "A two-steps prevention model of ATM frauds communications". Dept. of Computer Sciences Higher Colleges of Technology Abu Dhabi, UAE, 2018.

[9] J.J.Patoliya, M.M. Desai, "Face Detection based ATM Security System using Embedded Linux Platform ", 2nd International Conference for Convergence in Technology (I2CT), 2017.

[10] C. Bhosale, P. Dere, C. Jadhav, "ATM security using face and fingerprint recognition", International Journal of Research in Engineering, Technology and Science, Volume VII, Special Issue, Feb 2017.

[11] K. Shailaja and Dr.B.Anuradha, "Effective Face Recognition using Deep Learning based Linear Discriminant Classification ", IEEE International Conference on Computational Intelligence and Computing Research, 2016.

[12] M.Karovaliyaa, S.Karediab, S.Ozac, Dr.D.R.Kalbande, "Enhanced security for ATM machine with OTP and Facial recognition features",International Conference on Advanced Computing Technologies and Applications ,2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)