iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VII **Month of publication:** July 2020

DOI: https://doi.org/10.22214/ijraset.2020.30444

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: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

Card-Less ATM Transaction using Biometric and Face Recognition– A Review

Manish C M[1], N Chirag[2], Praveen H R[3], Darshan M J[4], D Kasim Vali[5]
[1, 2, 3, 4, 5]*Department of Computer Science and Engineering Vidyavardhaka College of Engineering, Mysuru, Karnataka India*

Abstract: ***Attacks on the Automated Teller Machine (ATM) has increased dramatically over the past decade which has inspired the utilization of biometrics with picture for individual distinguishing proof to obtain elevated level of security and precision. The task depicts a framework that replaces the ATM cards and PINs by the physiological biometric unique finger impression confirmation and face acknowledgment. Also, the element of one-time secret key (OTP) bestows security to the clients and liberates him/her from reviewing PINs. In this framework during enlistment the authentic client's unique finger impression and face is held in the database. The procedure of exchange starts by catching and coordinating fingerprints and face designs. The framework will naturally recognize genuine real attribute and phony examples. A GSM module associated with the Microcontroller will send a 4-digit code (OTP) created by the framework to the enrolled portable number. After the substantial OTP is entered the client can perform banking exchange. In any sort of phony access endeavors the record is blocked and the picture of the individual will be caught and transmitted by means of email.***

Keywords: ATM, Biometric, Fingerprint authentication, Face recognition, Face patterns, PINs, GSM, OTP.

I. INTRODUCTION

ATM can be depicted as Any Time Money. We can get cash at whenever anyplace just through ATM machines. To do the safe exchanges we need biometric validation. Biometric verification is a developing and dubious field. Today biometric laws and guidelines are in process and biometric industry principles are being tried. As indicated by, there are three well known assaults against ATM: Skimming, PIN logging and Integrity infringement. There are likewise assaults against cell phone: Fake versatile applications establishment, key logging programming and get PIN number during transmission. Other than that, an assault may likewise be a blend of the two kinds of said assaults.

Data likewise can be abused by a side channel assault. It is discovered that aggressors attempt to get the client's record data that put away on the attractive strip present at the rear of ATM card. Secret word is the main character that can use to validate the proprietor of ATM card. It implies anybody can get to the record bank through ATM machine as the secret key entered is right. Thus, when the ATM card and secret word is lost or taken by anybody, they can pull back the cash from that account effectively without the issue of client verification.

In this way, it can see that the most major issue brought up in ATM card security is about client verification. Client validation is significant on the grounds that it prompted the respectability infringement of financial balance data. It appears that this issue is more regrettable as anybody can get to all data put away when they entered the right secret word towards getting to ATM card at ATM machine. Other than that, it is firmly stressed that the security issues need innovation upgrades and better security strategy as a countermeasure.

In the first place, the financiers gather clients' fingerprints, facial ID and versatile numbers while opening records, at that point client just access ATM machine. The working of the ATM machine is with the end goal that when a client places a finger on the unique mark module it consequently checks to give approval for the exchange and its followed by a face acknowledgment. What's more, when both are looked at, it at that point naturally creates each time diverse 4-digit code as a message to the portable of the approved client through GSM modem associated with the microcontroller. The code got by the client is gone into the ATM machine by squeezing the keys on the touch screen. In the wake of entering it checks whether it is a substantial one or not and permits the client further access.

Biometrics can be characterized as quantifiable physiological and social trademark that can be caught and, in this manner, contrasted and another case at the hour of confirmation. It is mechanized techniques for perceiving an individual dependent on a physiological or social trademark.

©IJRASET: All Rights are Reserved

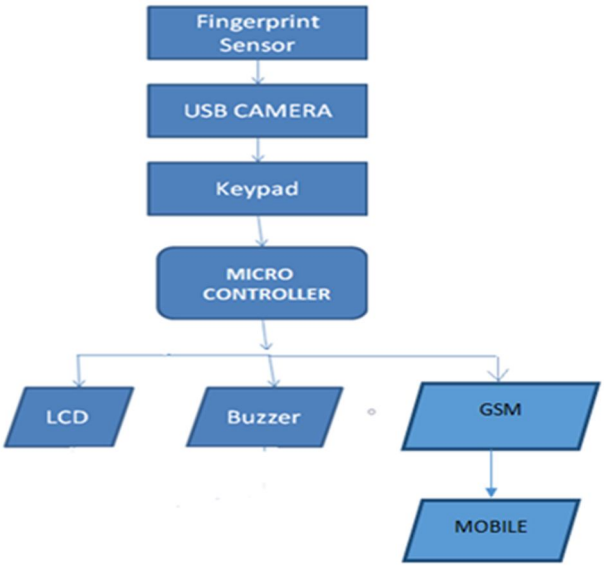


Figure 1.1 Flowchart of the working model

II. LITERATURE SURVEY

This paper refers on how to enhance security of transactions in ATM system using fingerprint and to develop ATM simulator-based fingerprint verification operations in order to reduce frauds associated with the use of Automatic Teller Machine [1]. This proposes a business model which helps the society, mainly the rural people who are less educated, by enhancing the security using Fingerprint recognition in Digital image processing and it has an additional feature i.e., a reference fingerprint of the nominee or a close family member of the customer can be used if the customer is not available in case of emergencies [2]. To provide secure system it collects multiple fingerprints of a same person. To obtain such result the fingerprint data in the form of two finger images as thumb and middle finger data and three finger images as thumb, middle and ring finger have been collected and combined by averaging to obtain another unique identity [3]. This proposed system was based on a prototype developed and the results were analyzed in Nigeria. The developed prototype was tested by Ten respondents who are users of ATM cards in the country and the data collected was analyzed using Statistical Package for Social Science (SPSS), and by the results the prototype can reduce the alarming rate of ATM fraud [4]. The method proposed in this paper focuses on how the money transaction in an ATM machine will be secured by providing personal identification by analyzing biometrics like fingerprints and iris patterns which are known for their steadiness and diversity. Use of biometrics provides a paperless banking environment along with the smart ATM access [5]. The proposed system solves sensor performance issue by adding a limit on amount of cash and number of transactions is defined in such a way that if one need to withdraw a big amount or attempts for multiple transactions by withdrawing small amount again and again, it shall be necessary to present biometric. On the other hand, if one need to make only balance enquiry or the cash is low and the number of transactions in a day is less than defined attempts, biometric presentation is not mandatory. Thus, it helps user to save time and maintain sensor performance by not furnishing their biometric for few hundred apart from maintaining security [6]. This paper evaluates the role of biometrics in human-machine interactions in applications such as decision-making, interview support systems and human-robot interfacing. Presently, there are biometrics projects that utilize the “talking face” technology. We forecast that future systems will verify humans using their biometrics, analyze facial expressions, temperature and blood pressure of the human, as well as generate cognitive questions and analyze answers [7]. This paper proposes an ATM system using biometrics like fingerprint, iris etc. During each transaction it checks whether the it is legitimate or not. Thus, improving the security of the system using biometric technology [8]. This paper presents a study of various ideas and translations of biometric quality so an away from of the current state and future headings can be introduced. A few factors that cause various sorts of debasements of biometric tests, including picture includes that credit with the impacts of these corruptions, are discusses in this paper [9]. This paper proposes a system for a forgotten card at the time of cash withdrawal. It can be overcome by using the face detection and recognition methods through ATM’s in-built camera [10]. This paper proposes a new ATM terminal customer recognition system which solves the problem of old system by using a chip of S3C2440 for the core of microprocessor in ARM9, an improved algorithm of fingerprint image which increases the security of the customers [11].

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

III. SYSTEM ANALYSIS

This gives a fundamental thought on how the current framework functions and furthermore gives an essential thought on the proposed framework conquered the detriments of the current framework.

A. Existing System

The present-day ATMs are utilizing pin-based security. At the point when we are going to complete the exchange, the pin number is taken care of as the information which is scrambled at the customer side and the information is decoded at the server side. At the point when the correlation gets fulfilled, we can complete the exchange. As the innovation is getting improved, the saltines are effectively recovering the information and subsequently the fakes are continuing expanding. The information is made accessible on cloud, with the goal that the exchange time gets diminished. At the point when the information is accessible in the cloud, information can be effectively recovered for false movement, which is the greatest disadvantage. Consequently, the best way to make sure about the datum is to supplant the PC produced numbers with the biometric security.

The current ATM framework confirms exchanges by means of the card and PIN-based framework. From that point, its awards access to bank clients to a few administrations, for example, money withdrawal and stores, record to account moves, balance enquiry, top-up buys and service charges installment. The ATM framework looks at the PIN entered against the put away approval PIN for each ATM clients. In the event that there is a match, the framework confirms the client and awards access to all the administrations accessible by means of the ATM. In the event that there is a confound then again, the client verification process comes up short and the client is given two additional chances to enter a right PIN. In the event that an off-base PIN is entered for the third time, the card gets blocked and held by the ATM.

An occasion of money withdrawal on the current ATM framework is portrayed in the progress outline in Figure. 1. Passage of a right PIN is satisfactory to confirm a client to the bank framework and from that point award access to the framework for withdrawal as delineated in Figure 1. The existing system retains Automated Teller Machine (ATM) cards after entry on an incorrect PIN of about three times, the system automatically eliminates further attempts to gain access as it is unauthorized.

B. Proposed System

These days we are utilizing the pin number for security in ATMs, which supplanted signature-based framework. The pin-based security is the easiest degree of security. The pin number is a one of a kind number which is scrambled and decoded during exchange. These days the pin number can be extricated through numerous ways, for deceitful action. Along these lines, as an answer the pin number can be supplanted with biometric security and facial acknowledgment.

In this framework during enlistment the veritable client's unique mark and face is held in the database. The procedure of exchange starts by catching and coordinating fingerprints and face designs. The framework will naturally recognize genuine real characteristic and phony examples.

IV. MODULE DESCRIPTION

The creators offer thanks towards the help gave by our tutors and employees who guided us all through the examination and helped us in accomplishing wanted outcomes.

A. Fingerprint Module

Startek FM220 is a CMOS-based optical peruse with high-caliber. It can catch pictures and check fingerprints with rapid. This can be utilized in both biometrics for security in unique mark recognition just as check. Startek FM-220 has utilized in enlistment and participation confirmation applications as an independent or installed gadget.

©IJRASET: All Rights are Reserved

B. Facial Recognition Module

Inbuilt delicate amplifier and picture sensor great CMOS sensor. Picture goal introduced to 25 super pixels with 6 light sensors. Picture control shading immersion, splendour, sharpness and brilliance is movable; Snap shot switch for taking despite everything pictures. Against glint 50Hz, 60Hz or open air; Resolution equipment: 500K pixels; Image quality: RGB24 or I420. Presentation: Auto or manual and edge of view: 58 Degree; Interface: USB2.0; Frame rate: 30 fps (max).

C. OTP Services

For actualizing OTP, we will utilize GSM modem to send SMS (an OTP) to client's portable number. The plan to utilize cell phones is favoured over email in light of the fact that the individuals in country zones have basic telephones which can get instant messages yet have no web associations and email offices. Since cell phones are pervasive, we plan to utilize cell phones so everybody can take the advantage of the new proposed framework. The client will get OTP following breezing through the face acknowledgment assessment. Once OTP is gotten client needs to enter the code which is of 6-digit. Client gets three opportunities to enter the code. In the event that the code is entered erroneously in three back to back endeavours account gets briefly blocked and notice is sent to enlisted versatile number. This component is included request to limit the fake methods for assaulting the record of a client by wearing veils or in uncommon cases, if unapproved client's face erroneously coordinates approved client's face.

V. RESULTS AND DISCUSSION

The proposed project which we have developed is an IoT oriented project which is first of its kind that is implemented for ATM transaction. The project involves Enrolling the customers data into the database. Here, the customer data is their name, email address, fingerprint, Facial data for authentication in Login page and Initial deposit. Secondly, we have the login page, where, the registered customers can Login by providing their fingerprint, Facial Recognition and followed by OTP pin which is sent to their mail. At last, we have an admin page, where, we can manage the registered users.

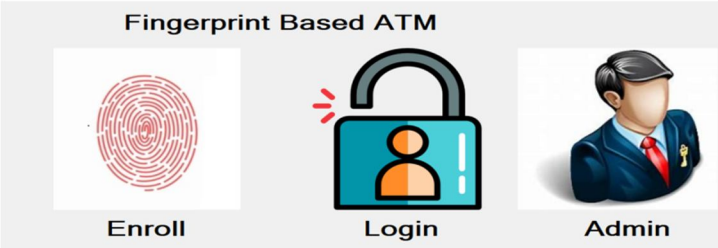


Fig 1: Home Page.

Fig 2: Admin Login Page.

©IJRASET: All Rights are Reserved

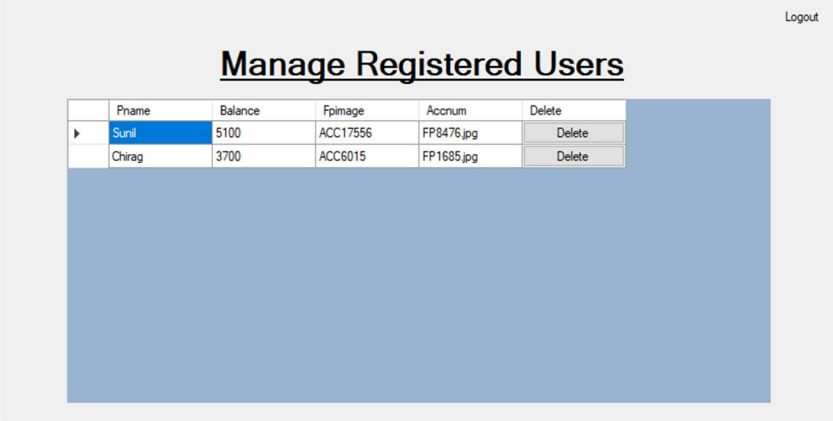


Fig 3: Managing Registered Users.

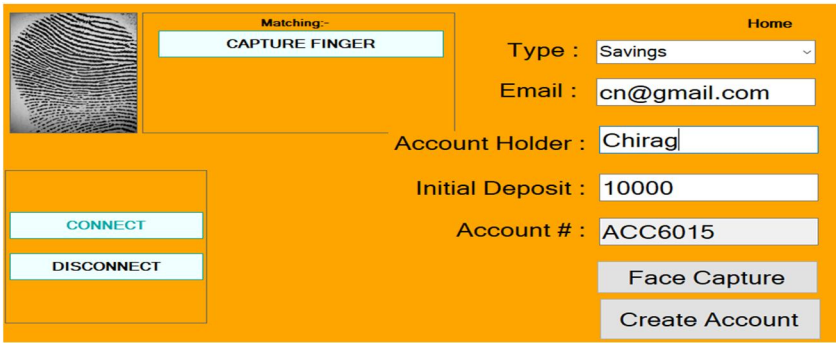


Fig 4: Creating new bank account in Enroll portal.

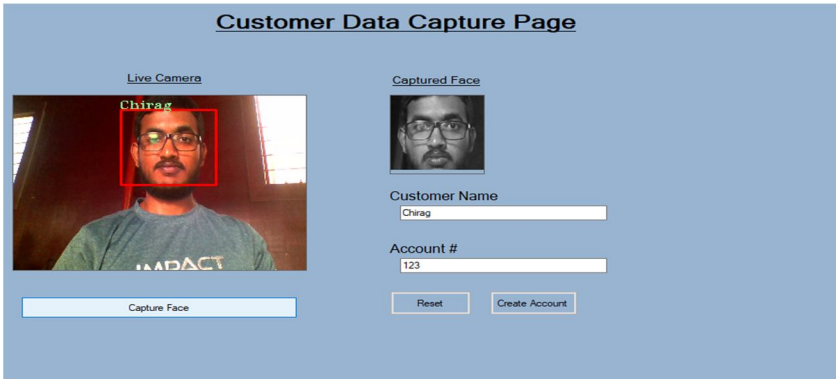


Fig 5: Capturing customer's face in Enroll portal.

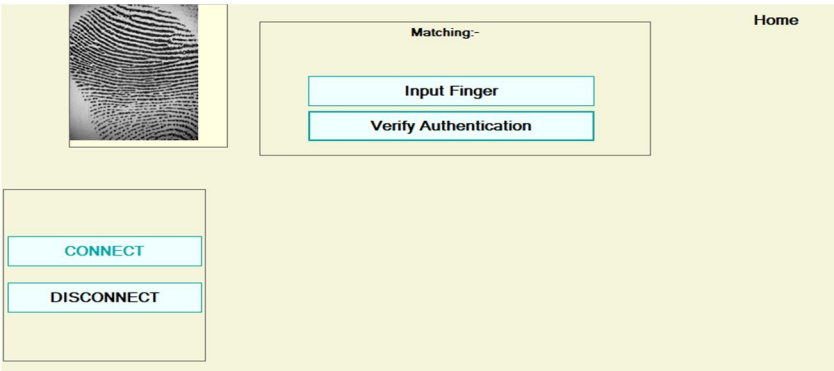


Fig 6: Authenticating customer's fingerprint in Login portal.

©IJRASET: All Rights are Reserved

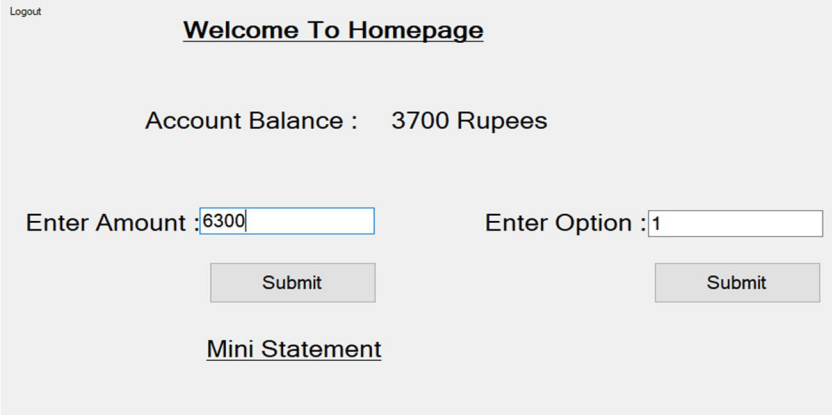


Fig 7: Banking interface after successful authentication.

VI. CONCLUSION AND FUTURE SCOPE

The utilization of the biometrics has made the ATM exchange framework progressively dependable and made sure about. The OTP and face acknowledgment idea added to the framework further improves the security and maintains a strategic distance from the need to recollect passwords. Besides, the framework is based on inserted innovation which makes it easy to understand and non-obtrusive. The time taken for the general ATM exchange is decreased for every client in contrast with the customary ATM exchange frameworks. Contrasting the proposed framework and the past ATM exchange frameworks, it shows that the precision and security of the proposed framework is greatest and progressively productive. The proposed framework gives more noteworthy level of security and comfort to the clients for simple, quick and Card-less ATM exchanges.

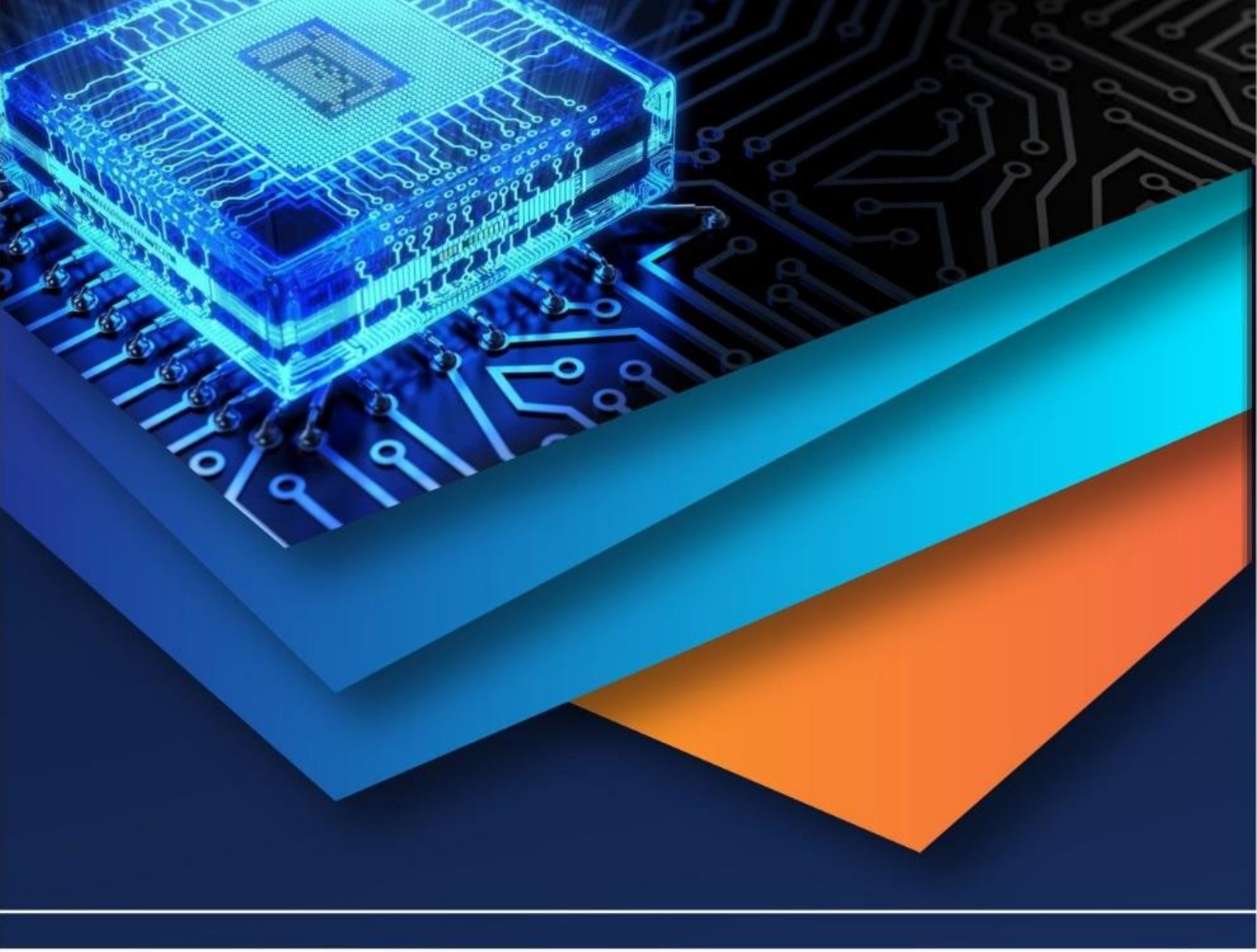
VII. ACKNOWLEDGEMENT

The creators offer thanks towards the help gave by our coaches and employees who checked us all through the examination and helped us in accomplishing wanted outcomes in given time.

REFERENCES

[1] Oko, S. and Oruh, J. (2012): Enhanced ATM security system using biometrics. IJCSI International Journal of Computer Science Issues, September 2012. Vol. 9, Issue 5, No 3, pp. 352-357.
[2] Ravikumar, S., Vaidyanathan, S., Thamotharan, S. & Ramakrishan, S. (2013), A new business model for ATM
[3] Maninder Singh, Shahanaz Ayub and Raghunath Verma, “Enhancing Security by averaging multiplefingerprint images,” Proc. International Conference on Communication Systems and Network Technologies, IEEE 2013.
[4] Jimoh, R.G. and Babatunde, A. N. (2014). Enhanced Automated Teller Machine using Short Message Service authentication verification. World Academy of Science, Engineering and Technology. International Journal of Computer, Information Science and Engineering 2014. Vol:8 No:1 pp.14-17
[5] Joyce Soares, A. N.Gaikwad “A Self Banking Biomtric M/C with Fake Detection Applied to Fingerprint and Iris along with GSM Tech. for OTP,” International Conference on Communication and Signal Processing, April 6-8, 2016,India.
[6] Shweta Singh , Akhilesh Singh, Rakesh Kumar, “A Constraint- based Biometric Scheme on ATM and Swiping Machine,” 2016 International Conference on Computational Techniques in Information and Communication Technologies(ICCTICT).
[7] W. A. Shier, S. N. Yanushkevich “Biometrics in Human-Machine Interaction,” The International Conference On Information and Digital Technologies2015.
[8] G. R. Jebline, S. Gomathi,” A Novel Method to Enhance the Security of ATM using Biometrics”, 2015 International Confernce on Circuit, Power and Computing Technologies [ICCPCT].
[9] Samarth Bharadwaj, Mayank Vatsa* and Richa Singh, “Biometric quality: a review of fingerprint, iris,and face,”Bharadwaj et al. EURASIP Journal on Image and Video Processing2014,2014:34http://jivp.eurasipjournals.com/content/ 2014/1/34
[10] Ekberjan Derman#1, Y. Koray Gecici#2, Albert Ali Salah*, “SHORT TERM FACE RECOGNITION FOR AUTOMATIC TELLER MACHINE (ATM) USERS,” 978-1-4799-3343- 3/13/$31.00 ©2013IEEE.
[11] Yun Yang , JiaMi, “ATM terminal design is based on fingerprint recognition,” 978-1-4244-6349-7/10/$26.00 ©201 0 IEEE.

©IJRASET: All Rights are Reserved



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)