iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8333

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:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Secured ATM Transaction Using SteganoPIN

M. Priyanka[1], T. Ravi Theja[2]
[1]*MTech, Embedded System* , [2]*Assistant Professor, Department of ECE,*
Malla reddy engineering college, Hyderabad, India

Abstract: The main objective of the project is to design "Secured ATM transaction using SteganoPIN". Users generally use the same personalized identification number (PIN) for multiple systems and in various sessions. Direct PIN entries are extremely at risk of shoulder-surfing attacks as attackers can effectively observe PIN entry with hidden cameras. To attain security and usability, we present a sensible indirect PIN entry technique called SteganoPIN, designed to physically block shoulder surfing attacks. In the basic user interface of SteganoPIN, one numeric keypad is a standard keypad in regular layout and the other in a random layout called the challenge keypad. The challenge keypad varies according with the ultrasonic sensor. A user must use this challenge keypad to derive a fresh OTP, the derived OTP is then entered on the response keypad. For each and every PIN entry the system captures the user's image by using UVC camera and sends it to registered mail ID.

I. INTRODUCTION

A. Personalized Identification Number Entry Security Issues

Personal identification numbers (PINs), generally constructed and memorized, are widely used as numerical passwords for user authentication or numerous unlocking purposes. Their application is increasing as a result of modern touch screens can facilitate convenient implementation of the PIN entry interface on a variety of commodity machines and devices, including automated teller machines (ATMs), point-of-sale (POS) terminals, debit card terminals, digital door-locks, smart phones, and tablet computers.

Unfortunately, when a user directly enters a secret PIN into such systems, security is easily compromised, significantly in public places. Nearby people can observe PIN entry by shoulder-surfing with or without hidden cameras. The human-only shoulder-surfing attacker is defined as a weak adversary who has no automatic recording device, however might use manual tools like a paper and pencil. The perceptual and cognitive capabilities of human-only attackers are confined to those of humans. The camera-based shoulder-surfing attacker is defined as a stronger adversary assisted by an automatic recording tool, like a wearable camera, to record and analyze entire transactions effectively even at long range .

Moreover, adversaries who have already mounted shoulder-surfing attacks and collected multiple PIN candidates can attempt to impersonate a user. The active-guessing attacker is an adversary who makes an attempt guesses with PIN candidates. Such an attacker will become more powerful when she repeats camera-based observation of identical user and system. Remote connected observation is additionally turning into a priority as a result of high-resolution cameras are being distributed and networked in public places. The recent trend of targeting attacks and the advent of wearable computers make continual camera-based shoulder surfing attacks an more and more realistic threat to the PIN user interface.

The number of PIN candidates should stay sufficiently large to scale back data leakage even if a user's PIN entries are repeatedly observed by adversaries. Even partial information leakage can be harmful because users generally reuse identical or a minimum of similar PINs for multiple systems. Furthermore, a token and/or ID usually combined with a PIN can be pick pocketed or skimmed by adversaries using alternative physical channels. Thus, once a secret PIN is compromised, a user can be exposed to multiple breaches of security.

B. Security-Improved Personalized Identification Number Entry Measures: Related Work

To take care of these nontechnical attacks, one promising intervention is through the user interface. the main aspect has been incorporating indirect key entry measures to separate the visible keyed entry components from the secret ones.

Earlier analysis with passwords investigated cognitive authentication within the constraints of humans. Roth et al. Used two colors for indirect PIN entry within the technique we tend to call Binary PIN. In every round, the system colored a random half of the numeric keys black and therefore the other half white thus users may enter the color of the PIN key by pressing a separate color key. Multiple rounds were played to enter one digit of the PIN and repeated till all PIN digits were entered. Wiedenbeck et al. presented the convex hull click (CHC) for graphical passwords. In CHC, the long-run secret was pass-icons, and a random challenge used a number of random-located icons together with both pass and fake icons. For authentication, users created a image of a convex hull linking pass-icons and clicked inside during multiple rounds. Weinshall introduced the cognitive authentication theme (CAS) for graphical passwords. In CAS, a random challenge was a collection of pictures together with a password and fakes, randomly

organized on a table. Users derived a visible path based on the password pictures on the table and entered its destination value in multiple rounds. de Luca et al. presented Color PIN, that used a collection of colored characters as a random challenge assigned to numeric keys on a keypad. In every round, three different-colored characters were assigned to every numeric key whereas each character was duplicated on three numeric keys in several colors. In Color PIN, the secret PIN was really color-digit combinations. The user entered a secret-colored character of a PIN key using a separate alphabetic keyboard repeatedly till the entire PIN was entered. Major considerations with these strategies are longer authentication time and longer passwords to recollect. Others additionally raised security considerations.

To address camera-based shoulder-surfing attacks over multiple authentication sessions and to migrate users already aware of the standard PIN entry system, this paper presents a unique PIN entry method referred to as SteganoPIN.

The SteganoPIN system builds on the idea of challenge-response rendered over a user interface and to advance the following goals for PIN-based authentication.

1) *Usability:* Should use the regular numeric keypad for key entry. Should incur restricted increases in PIN entry time and error rates. Should increase the length of a long-run PIN. Should stay within the short-term memory requirements of human limitations like four groups of items.
2) *Strong Security:* should be resilient to camera-based shoulder surfing attacks over multiple authentication sessions. Should resist active guessing attacks without permitting additional advantage than random guessing.

II. PROPOSED SYSTEM

To achieve security and usefulness, we present a sensible indirect PIN entry method referred to as SteganoPIN. The SteganoPIN for secured ATM transaction is a two numeric keypads, one covered and the other open, designed to physically block shoulder surfing attacks. After locating a long-run PIN within the additional typical layout, through the covered permuted keypad, a user generates a one-time PIN that may safely be entered in plain view of attackers.

Here we are using Raspberry Pi board, ultrasonic sensor and Camera.

A. *Block Diagram*

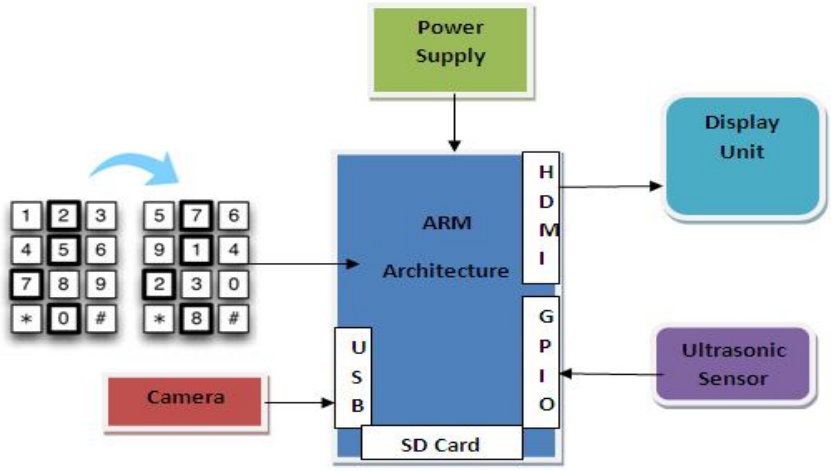


Figure 1: Block Diagram

III. HARDWARE IMPLEMENTATION

A. *Raspberry Pi Board*

The Raspberry Pi is a credit card sized single-board computer developed in the UK by the Raspberry Pi. Foundation with the intention of promoting and teaching of basic applied science in schools. The Raspberry Pi has a Broadcom BCM2387 chipset, which has an 1.2GHz Quad-Core ARM Cortex-A53 (64Bit) processor, twin Core Video Core IV multimedia Co-Processor with 1GB of RAM. It doesn't include a inbuilt hard disc or solid-state drive, however uses an SD card for booting and persistent storage.

Figure 2: Raspberry Pi Board

The Raspberry Pi 3 has four built-in USB ports provide enough connectivity for a mouse, keyboard. On top of all that, the low-level peripherals on the Pi make it great for hardware hacking. The 40-pin header on the Raspberry Pi gives you access to 27 GPIO, UART, I2C, SPI as well as 3.3 and 5V sources. The Broadcom BCM2837 system-on-chip (SOC) includes four high-performance ARM Cortex-A53 processing cores running at 1.2GHz with 32kB Level 1 and 512kB Level 2 cache memory, a Video Core IV graphics processor, and is linked to a 1GB LPDDR2 memory module on the rear of the board.

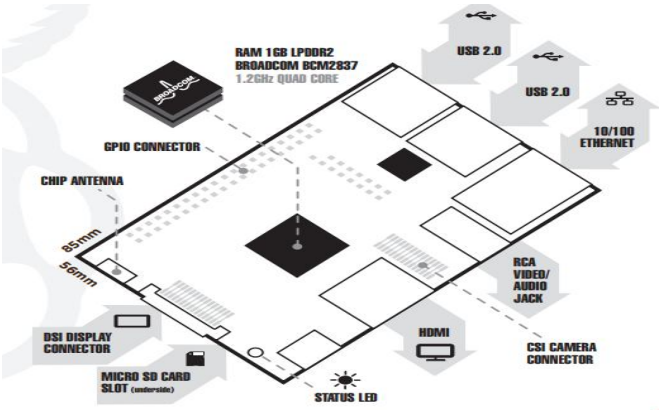


Figure 3: Raspberry Pi Board features

B. UVC Driver Camera

Figure 4: UVC Drive camera

A UVC (or Universal Video Class) driver is a USB-category driver. A driver permits a tool, like your digital camera, to speak together with your computer's OS. And USB (or Universal Serial Bus) may be a standard form of connection that enables for high-speed data transfer. Most current operative systems support UVC, though UVC may well be a relatively new format, it's quickly becoming common. In different words, with a UVC driver, you'll be able to simply plug your digital camera into your laptop and it'll be ready to use.

There are 2 forms of digital camera drivers

1) The one enclosed with the installation disc that came together with your product. For your digital camera to work properly, this driver needs a while to place in. it's specifically tuned for your digital camera, designed by your digital camera manufacturer and optimized for digital camera performance.]
2) A UVC driver:-You can only use one driver at a time, but either one will alter you to use your digital camera with varied applications.

IV. SOFTWARE REQUIREMENTS

A. *LINUX Operating System in Operation System*

Linux is also a free and open source software for computers. The operating system could be a collection of the essential instructions that tell the electronic components of the computer what to do and the way to work. Free and open source software (FOSS) implies that everybody has the liberty to use it, see how it works, and changes it. There is lot of code for Linux operating system, and since Linux operating system is free code it implies that none of the code will place any license restrictions on users. This is often one of the reasons why many people choose to use Linux operating system.

A Linux-based system is a standard Unix-like operating system. It derives a lot of its basic design from principles established in UNIX during the Seventies and Eighties. Such a system uses a monolithic kernel, the Linux kernel, that handles process management, networking, and peripheral and file system access. Device drivers are either integrated directly with the kernel or else as modules loaded while the system is running.

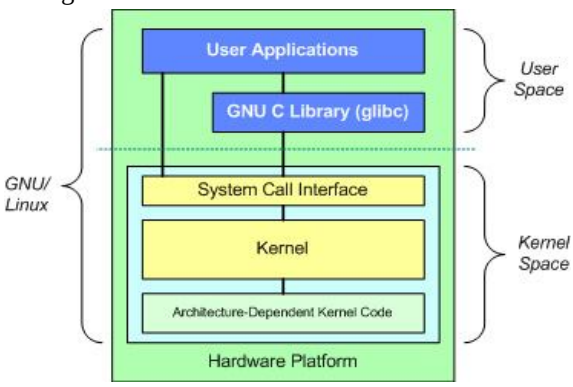


Figure 5: Architecture of Linux Operating System

B. *Qt for Embedded Linux*

Qt is a cross-platform application framework that's wide used for developing application software with a graphical user interface (GUI) (in that cases Qt is classified as a widget toolkit), and additionally used for developing non-GUI programs like command-line tools and consoles for servers. Qt uses normal C++ however makes extensive use of a special code generator along with many macros to enrich the language. Qt may also be employed in many different programming languages via language bindings. It runs on the main desktop platforms and a few of the mobile platforms. Non-GUI options include SQL database access, XML parsing; thread management, network support, and a unified cross-platform application programming interface (API) for file handling.

C. *Open CV Library*

Open CV (Open supply pc Vision) consists of set of library functions for programming, for real time pc vision. it's developed by Willow Garage, that's in addition the organization behind the illustrious golem OS (ROS). Currently you'd say MATLAB may do Image process, then why open CV? Some distinction between MATLAB and openCV

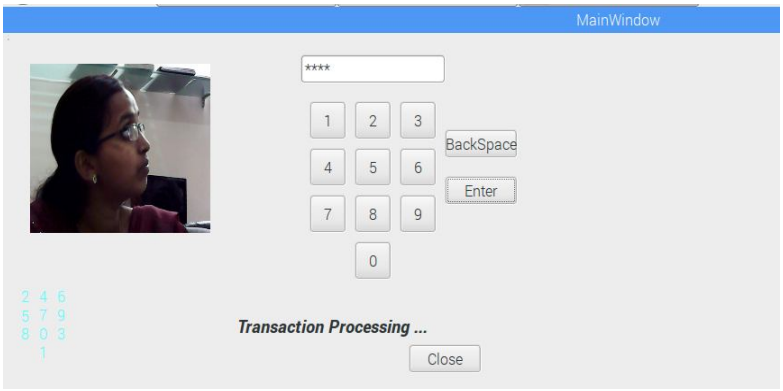
Speed: MATLAB is created on Java, and Java is created upon C. thus once you run a MATLAB program, your pc is busy creating an effort to interpret all that MATLAB code. Then the code is decoded into Java, then solely the ultimate code is dead. Whereas, AN Open CV consists a library functions written in C/C++. You are nearer to directly supply machine language code to the pc to urge dead. As a result of this, programs written in Open CV run lots of faster than similar programs written in MATLAB.

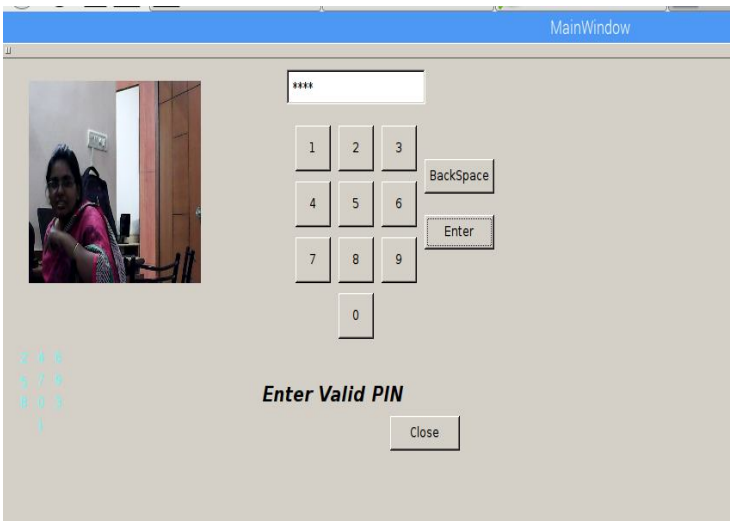
Resources needed: MATLAB uses innumerable system resources, because it is of high level in nature. To run a video it needs over a GB of RAM. Whereas, AN OpenCV needs approx 70MB of RAM.

Cost: price for the bottom MATLAB is around USD 2150. Open CV is free.

Portability: MATLAB and Open CV run well on. Windows, Linux and mackintosh OS. However AN Open CV, can run on any device that runs C.

V. RESULT



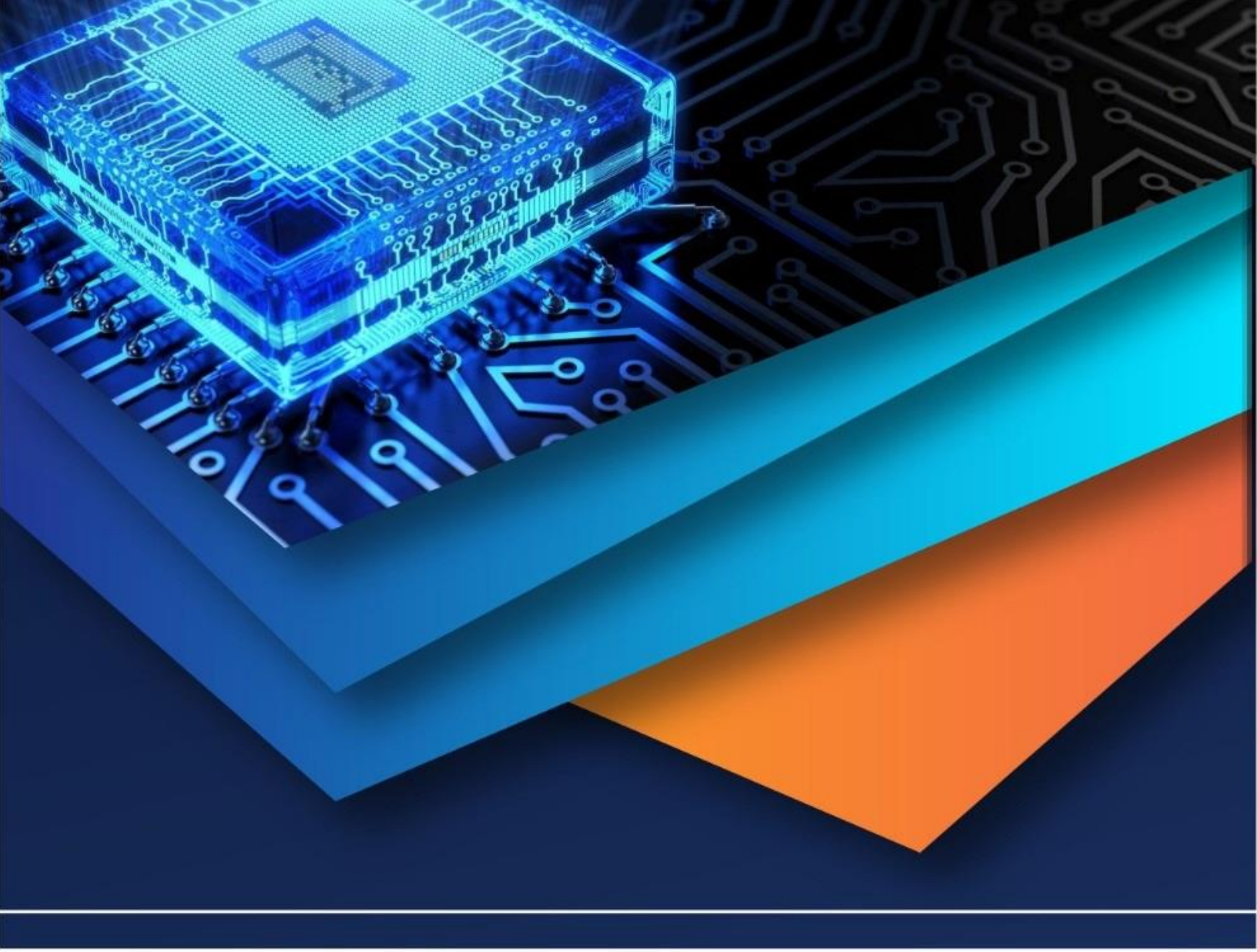


VI. CONCLUSION

The project "Secured ATM Transaction using SteganoPIN" has been with success designed and tested. it's been developed by desegregation options of all the hardware parts and computer code used. Presence of each module has been reasoned out and placed rigorously so contributory to the most effective operating of the unit. Secondly, extremely advanced Raspberry pi board and with the assistance of growing technology the project has been successfully implemented.

REFERENCES

[1] J. Long and J. Wiles, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Boston, MA, USA: Syngress, 2008.
[2] A. Greenberg. (2014, Jun.). Google glass snoopers can steal your passcode with a glance," Wired. [Online]. Available: http://www.wired.com/ 2014/06/google-glass-snoopers-can-steal-your-passcode-with-a-glance/.
[3] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in Proc. ACM Comput.Commun. Security, 2004, pp. 236–245.
[4] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 6, pp. 716–727, Jun. 2014.
[5] Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of designing leakage-resilient password systems: Attacks, principles and usability," in Proc. 19th Internet Soc. Netw. Distrib. Syst. Security Symp., 2012, pp. 1–16.
[6] A. Parti and F. Z. Qureshi, "Integrating consumer smart cameras into camera networks: Opportunities and obstacles," IEEE Comput., vol. 47, no. 5, pp. 45–51, May 2014.
[7] B. Song, C. Ding, A. Kamal, J. Farrell, and A. Roy-chowdhury, "Distributed camera networks," IEEE Signal Process. Mag., vol. 28, no. 3, pp. 20–31, Apr. 2011.
[8] A. De Luca, M. Langheinrich, and H. Hussmann, "Towards understanding ATM security—A field study of real world ATM use," in Proc. ACM Symp. Usable Privacy Security, 2010, pp. 1–10.
[9] J. Rogers, "Please enter your 4-digit PIN," Financial Services Technology, U.S. Edition, vol. no. 4, Mar. 2007.
[10] T. Matsumoto and H. Imai, "Human identification through insecure channel," in Proc. Adv. Cryptol., 1991, pp. 409–421.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY