iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69841

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 13 Issue IV Apr 2025- Available at www.ijraset.com

Intelligent Facial Authentication and Gate Control for Campus Safety Using Deep Learning

Mrs. Y. Anusha[1], P. Bhanu Sri[2], P. Greeshma Sri[3], P. Mohana Keerthi[4], Sk. Ture Sakhiba Banu[5]
[1]*MTech,* [2, 3, 4]*BTech, Computer science & Engineering, Bapatla Women's Engineering College, Bapatla, AP, India*

Abstract: ***This research presents an intelligent approach for authenticating student IDs. To ensure that students are who they say they are, it employs deep learning and facial mapping. You may now use your face instead of a physical ID card using this technique. Both the process's security and its convenience are enhanced by this. Access is granted via ID cards in conventional systems. These may be misplaced, taken, or abused. Using state-of-the-art technology, our solution resolves these issues. We use student face data to construct a deep learning model. At the entrance, a camera records the face of every student. Using a database comparison, the system verifies the current picture. The gate will open if the faces match. If it doesn't, the security team will get a notification. Regardless of the ambient light or the user's emotional state, the device performs well. Additionally, it is quick, precise, and doesn't need any physical touch. That means ID cards won't be needed as often. Additionally, it lessens the possibility of unlawful entry.***

I. INTRODUCTION

The fields of biology, statistics, and computer science all come together in one technological marvel. Simple statistical models were used by earlier systems. These days, sophisticated systems are dependent on deep learning and machine learning. Facial recognition is more secure and difficult to forge than other biometric authentication methods like iris or fingerprint scanning.

There are two parts to facial recognition: detecting faces and recognizing faces. One way to tell whether a face is there is by using detection. Facial recognition works by comparing the image of the subject to previously recorded info. Modern systems are capable of reaching an accuracy level of 99.15%, which makes the technology dependable for safe authentication. Following detection, the face's structure and proportions are examined. Lip and eye socket size, in addition to the distances between the eyes, nose, mouth, and jaw, are all factors that the system takes into account. It is possible to utilize many photos with various perspectives or emotions to increase precision. Facial recognition has the advantage of not requiring any physical touch. It actively records information about faces. Because of this, it is easier to utilize than alternatives, such as fingerprints or DNA. In everyday life, people see it as more natural and acceptable. Additionally, the device provides information on facial expressions and movement. It has multi-face detection and recognition capabilities, which come in handy in real life. Quick and easy user authentication is possible without the need for human verification. As a result, precision and speed are both enhanced. You may put it simply. Cameras can record faces on film. In order to identify a person, the algorithm takes their face and checks it against a database. Identity is verified if the match is more similar than a certain threshold. A subject faces the camera while verification is underway. They get a facial scan, which is then compared to their record. One major perk is that it may take place remotely, undetected by the target. One area where facial recognition really shines is in the realm of surveillance. Quick searches in massive datasets are made possible. Suspects, missing individuals, or known criminals may be located with this aid. Despite the fact that faces may be hidden, the technology remains a powerful tool for verification. Nevertheless, factors like as illumination, motion, and camera focus may impact precision. Enhancing performance may be achieved by integrating face recognition with other biometric technologies. When combined, they provide identifying systems that are both more secure and more effective.

II. LITERATURE SURVEY

A system for automatic face recognition and identification using OpenCV was created by D. Mary Prasanna et al.; it is GUI-based and runs in real-time. Feature extraction, recognition, and detection are the three phases that make up the system. The system is able to recognize faces in webcam images and extract 128 facial features by using a deep neural network approach. A support vector machine (SVM) classifier is then used to carry out the identification process. The system utilizes the Histogram of Oriented Gradients (HOG) approach to enhance the dimensionality reduction of face photographs. The average identification accuracy was 75% after testing with 60 pictures. The research skirts the topic of the Open Face tool's limitations, namely its sensitivity to changes in location and illumination, and fails to evaluate the system's performance with a large number of users or photographs.

An intelligent face recognition and identification system was presented by M. H. Khairuddin et al. for use in smart buildings. Both software and physical components make up the system. The hardware that can identify and detect human presence consists of a camera sensor and a Raspberry Pi 3. Software developers often work with HTML and cloud storage platforms like Dropbox to save user-taken images. Two instances of cloud storage, Dropbox and Cloudinary, were compared to measure the system's efficiency. When comparing performance, functionality, and picture quality, Dropbox came out on top.

A video-based face recognition attendance system is presented and compared by Anshun Raghuwanshi and colleagues. To reliably register student attendance from a video source, this system utilizes biometric face recognition technology. Before comparing a detected face to a database of student names and images, Face Detection is used to separate faces from other things. Then, Face Recognition is used. If there is a match, attendance will be noted on an Excel file. Using the ORL database with 400 photographs (10 per subject) and a class database with 25 photos (5 per person), experiments were done to test face recognition using the Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) techniques. While LDA attains an accuracy of 60% for the class database and an accuracy of 83.57% for the ORL database, PCA only manages 66.07% and 53.33%, respectively.

III. EXISTING SYSTEM

Utilize Conventional Cameras, Which Might Fail in Different Lighting Conditions.
Deals with problems that impact accuracy in lowlight.
No alert is generated for illegal people, even when face capture is conducted.

IV. PROPOSED SYSTEM

1) Facial Recognition Workflow: A picture or video input is required before the system can do face recognition. A camera or other image sensor is used for this purpose. For the camera and software to cooperate, their settings must be correct.
2) Input Stage: You may use either still photos or live video as input. The system starts to detect faces in the video once the input is given. The next step in the recognition process is to use trained classifiers.
3) Recognition Using Python: Various recognition tasks make use of different Python programs. These programs use the learned classifier to recognize people in both current and archived photos. To keep track of when a match is detected, the system records the timestamp.
4) Unrecognized Individuals: The device is designed to notify security personnel in the event that it identifies an unfamiliar face. Prior to admission, guests are given a unique QR code. Included in this QR code are the names of the host and visiting students, as well as the student ID. Scan it at the gate to get temporary admission and securely record your visit.
5) Monitoring Student Movement: A notification will be sent to the coordinator via the system if a student leaves the campus within permitted hours. The student's name and ID are included in this alert, allowing for real-time monitoring and intervention.
6) OpenCV and Facial Recognition: One flexible tool for face recognition that Gray Bradski suggested was OpenCV. With it, you get XML documentation and support for various operating levels. Body component analysis is only one example of the many non-facial recognition applications of OpenCV.
7) Deep Learning Integration: To improve accuracy, modern systems increasingly use deep learning. Face assessment is made better by deep metric learning, like the one used in dlib. Important components of this system are Dlib and the facial recognition library.
8) Python in Face Recognition: Because of its strength and ease of use, Python is often used for facial recognition and detection applications. When integrated with OpenCV and dlib, it greatly improves the efficiency and effectiveness of webcam-based real-time recognition.

A. Establishing a Facial Database

In order to construct a dataset of 30 pupils, a technique was devised for picture collection. At the beginning, each student has ten photographs, for a total of three hundred. Each student adds 100 more photographs to the total of 3000 by image augmentation methods such as flipping, cropping, and rotating. In doing so, it aids the deep neural network's learning process.

B. Face Detection

When detecting faces, the system employs the MTCNN model. MTCNN is a CNN that uses three stages—P-Net, R-Net, and O-Net—to remove background noise. In order to find the final face and important traits, it constructs a pyramid of picture scales, recognizes faces, and refines findings.

C. Face Recognition

Recognition is when FaceNet comes into play. In order to create 128-dimensional embeddings from faces, it employs a triplet loss function. In the feature space, this function makes sure that faces that are similar are closer together and faces that are distinct are further away. You may compare the finished embeddings by saving them in a.pkl file.

D. Saving Information

The system creates a CSV file with the student's name, arrival time, and date after a face is detected. When there isn't a match, a warning is sent out and the unknown face is saved with its timestamp.

E. Unauthorized Entry Alarm

Unrecognized entries are protected by an alert mechanism that is built in. An alert is activated with the use of Python's winsound module if a face does not match. In the event of an incursion, the adjacent personnel may be quickly alerted by the loud buzzer.

F. Coordinator Email Alerts

Using Python's smtplib, an email is sent to the coordinator if a student leaves the school during restricted hours. Coordinators can easily keep tabs on students and reply quickly thanks to the email, which contains their name and ID.

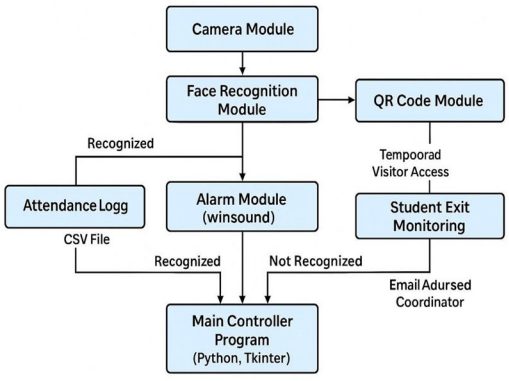
G. Visitor QR Code Access

A qrcode code generated by Python's qrcode module is sent to the visitors. Names of both the visitor and the student host, as well as the student ID, are included. To ensure the safety of the campus, scan this QR code at the entrance to get temporary, monitored entry.

V. MODULES

1) Face Data Collection: In order to build a face database, the system takes pictures of approved users (such students) and keeps them. To increase the dataset and the quality of the model, techniques such as picture augmentation are used.
2) Face Recognition: In order to identify a person, deep learning models (such as FaceNet) examine and compare stored data with faces captured in real-time video or photos. The individual is verified if the match is approved.
3) Gate Entry Authentication: The device at the entrance gate either grants or rejects admission based on facial recognition. This procedure is fully automated and requires no human intervention, making it more convenient and secure.
4) Access Control: Manages access to certain locations (like dorms for students). To enter, one must be either registered or have a QR code that verifies their identity.
5) Time Stamp: The precise moment and date of each arrival and departure is recorded. Accurate records and movement histories may be better tracked using this.
6) Notifications: The technology notifies security or designated personnel in real-time by email or alarm if a student leaves during restricted hours or if an unknown individual is discovered.
7) QR Code: Guests on a temporary basis are given QR codes that include their name, information about the host student, and the duration of their access. In order to maintain the campus's security, visitors may scan a QR code at the entrance to get restricted access.

VI. SYSTEM ARCHITECTURE



Gate Entry Face Recognition-Based Attendance and Security System

VII. RESULT AND ANALYSIS

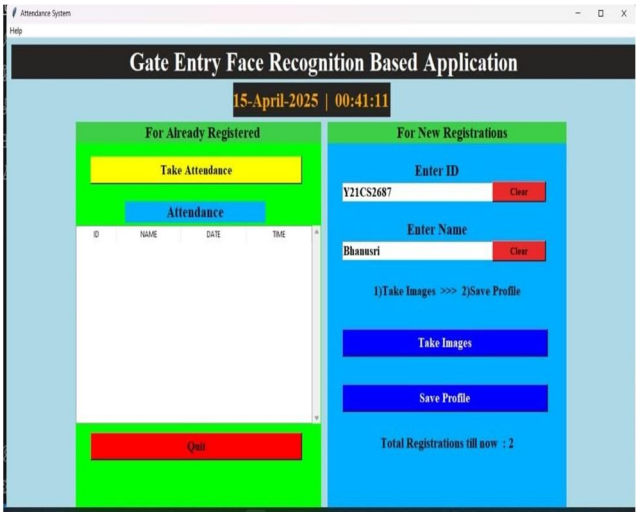


Fig 1: GUI Interface

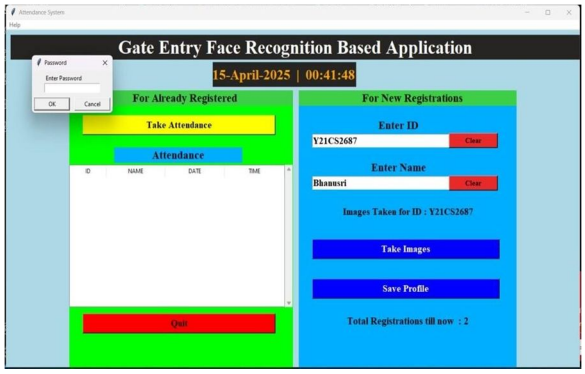


Fig 2: New Registrations

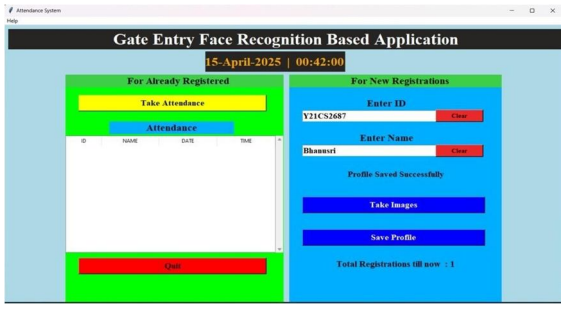


Fig 3: Stored in the database

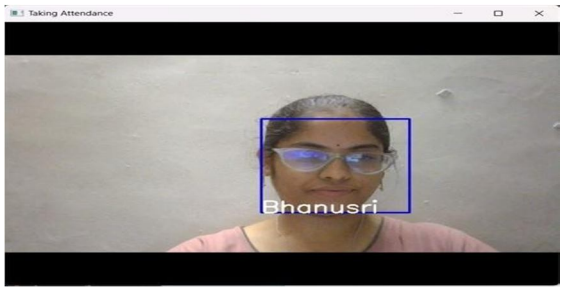
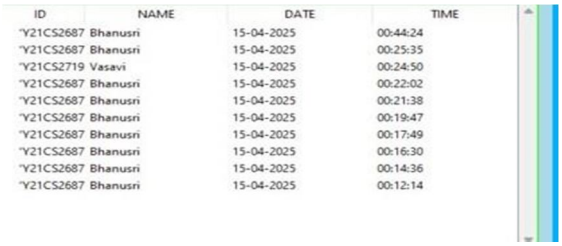


Fig 4: Face Recognizing with voice



ID	NAME	DATE	TIME
Y21CS2687	Bhanusri	15-04-2025	00:44:24
Y21CS2687	Bhanusri	15-04-2025	00:25:35
Y21CS2719	Vasavi	15-04-2025	00:24:50
Y21CS2687	Bhanusri	15-04-2025	00:22:02
Y21CS2687	Bhanusri	15-04-2025	00:21:38
Y21CS2687	Bhanusri	15-04-2025	00:19:47
Y21CS2687	Bhanusri	15-04-2025	00:17:49
Y21CS2687	Bhanusri	15-04-2025	00:16:30
Y21CS2687	Bhanusri	15-04-2025	00:14:36
Y21CS2687	Bhanusri	15-04-2025	00:12:14

Fig 5: CSV File

Fig 6: QR Code for visitors

Fig 7: QR Code Generator

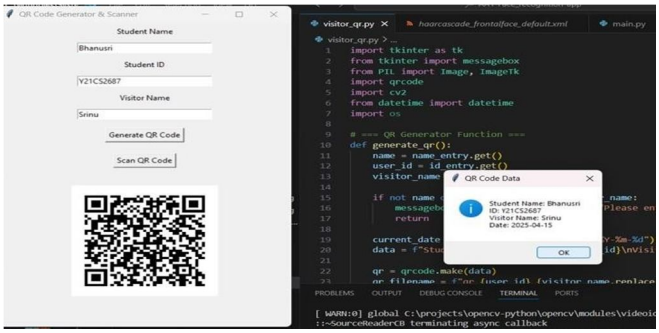


Fig 8: QR Code Scanner

Fig 9: Email to coordinators

VIII. CONCLUSION

A potential solution to the problems of accessibility and security in student housing might be an admission system that relies on facial recognition technology. They may assist keep dorms safe from intruders and expedite the entry and leave procedures. The ultimate goal of this study is to design a smart hall security system that can recognize faces in real-time by using intelligent face detection and recognition technology. A real-time face recognition system with detection and recognition capabilities, suitable to multiple security services, was created after this research studied numerous facial recognition algorithms. The system is simple to set up, affordable, and straightforward for users. Updating student datasets to make sure they are secure and accurate could be a part of future improvements. It is possible for security staff to get push alerts whenever an unfamiliar individual is identified. Furthermore, novel methods are needed to circumvent constraints and successfully identify many people in diverse settings.

IX. FUTURE SCOPE

Eventually, the system will be able to work without an internet connection at gate entrance points, enabling students to be authenticated and their timestamps to be logged. Parents will be notified instantly via a mobile app whenever a student enters or leaves the building.

REFERENCES

[1] Khairuddin, MH, and Shahbudin SK, Kassim M. "A Smart Building Security System with Intelligent Face Detection and Recognition." In IOP Conference Series: Materials Science and Engineering, 2021;1176(1):012030. IOP Publishing.
[2] Chauhan, M, and Sakle M. "Study & Analysis of Different Face Detection Methods." International Journal of Computer Science and Information Technologies, 2014;5(2):1615- 1618.
[3] Aydin, Ilhan, and Nashwan Adnan Othman. "A New IoT Combined Face Detection System Using Computer Vision for Security Application." In 2017 International Artificial Intelligence and Data Processing Symposium (IDAP), 2017;1-6. IEEE.
[4] Raghuwanshi, Anshun, and Preeti D. Swami. "An Automated Classroom Attendance System Using Video-Based Face Recognition." In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017;719-724. IEEE.
[5] 28. Soniya V, Swetha Sri R, Swetha Titty K, Ramakrishnan R, Sivakumar S. "Attendance Automation Using Face Recognition Biometric Authentication." In 2017 International Conference on Power and Embedded Drive Control (ICPEDC), 2017:122-127. IEEE.
[6] Yang, M. H., Ahuja, N., & Kriegman, D. (2000). Face detection using mixtures of linear subspaces. In Automatic Face and Gesture Recognition, 2000. Proceedings. Fourth IEEE International Conference on (pp. 70-76). IEEE.
[7] Yang, G., & Huang, T. S. (1994). Human face detection in a complex background. Pattern recognition, 27(1), 53-63.
[8] N.Stekas, D.Heuvel, “Face Recognition Using Local Binary Patterns Histograms (LBPH) on an FPGA-Based System on Chip (SoC),” IEEE, Chicago, IL, USA, Aug 2016.

AUTHOR'S PROFILES

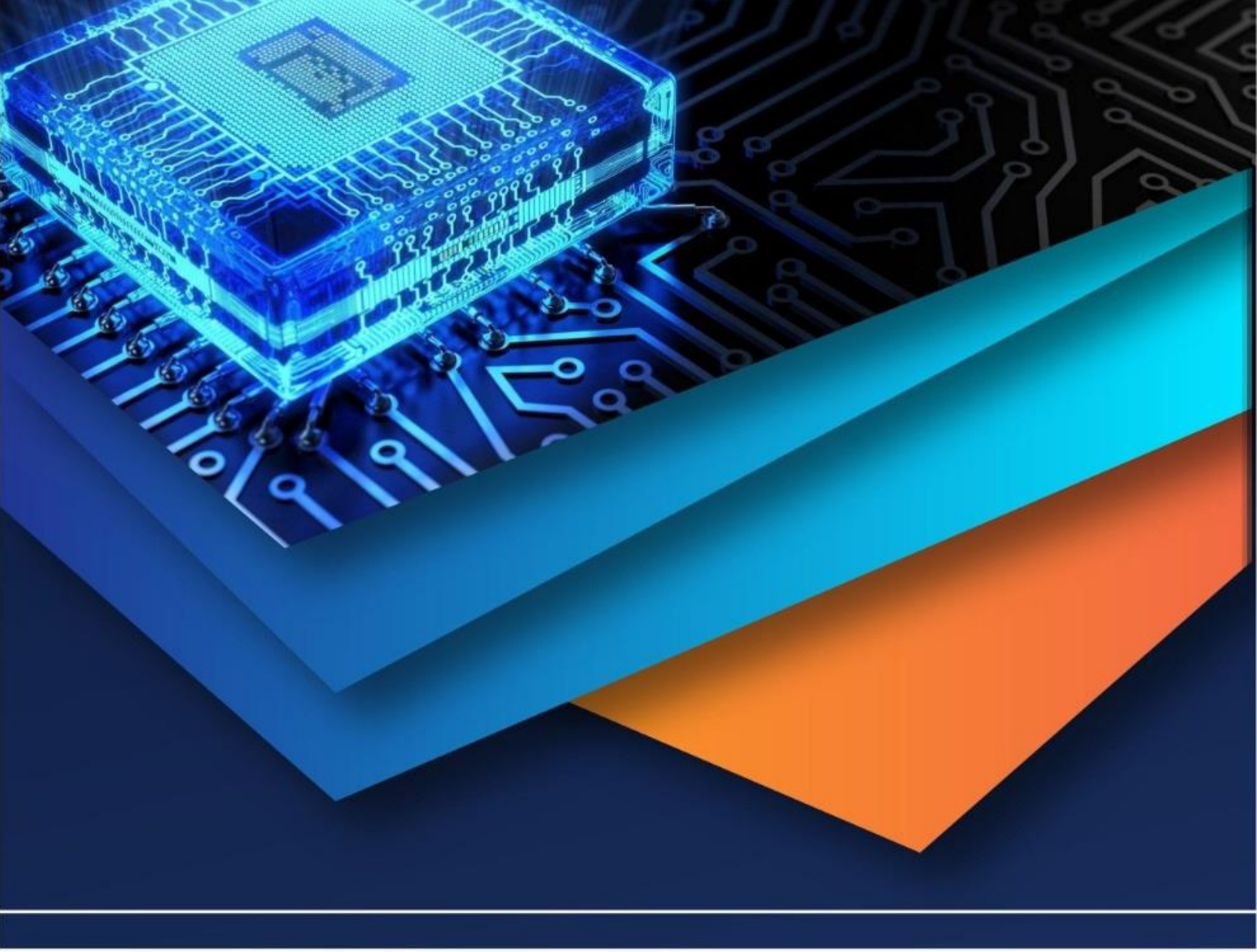
Mrs. Y. Anusha working as Assistant Professor in Department of CSE, BWEC, Bapatla.

P. Bhanu Sri B. Tech with specialization of Computer Science & Engineering in Bapatla Women's Engineering College, Bapatla.

P. Greeshma Sri B. Tech with specialization of Computer Science & Engineering in Bapatla Women's Engineering College, Bapatla.

P. Mohana Keerthi B. Tech with specialization of Computer Science & Engineering in Bapatla Women's Engineering College, Bapatla.

Sk. Ture Sakhiba Banu B. Tech with specialization of Computer Science & Engineering in Bapatla Women's Engineering College, Bapatla.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY