International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902011

Face Recognition Door Lock System with IoT &AI

D.Naresh[1], P.Anand[2] , M.Harish[3], A.Vamshi[4],A.Kethan[5], Mrs.B.Nirmala[6], Dr.M.Saravanan[7]

UG Student, B. Tech CSE 4thyear, Holy Mary Inst. of Tech. and Science, Hyderabad, TG, India[1]

UG Student, B. Tech CSE 4thyear, Holy Mary Inst. of Tech. and Science, Hyderabad, TG, India [2]

UG Student, B. Tech CSE 4thyear, Holy Mary Inst. of Tech. and Science, Hyderabad, TG, India [3]

UG Student, B. Tech CSE 4thyear, Holy Mary Inst. of Tech. and Science, Hyderabad, TG, India [4]

UG Student, B. Tech CSE 4thyear, Holy Mary Inst. of Tech. and Science, Hyderabad, TG, India [5]

Assistant Professor, Holy Mary Inst. of Tech. and Science, Hyderabad, TG, India [6]

Professor, Holy Mary Inst. of Tech. and Science, Hyderabad, TG, India [7]

Publication History: Received: 23.02.2026; Revised: 10.03.2026; Accepted: 13.03. 2026; Published: 18.03.2026.

ABSTRACT: This project presents an AI-Based Smart Door Unlock System using Face Recognition and IoT Integration, which provides a secure and automated access control solution. The system captures facial images using a camera, processes them through machine learning and computer vision techniques, and compares them with a trained image database of authorized users. If a valid match is found, access is granted; otherwise, access is denied and theattempt is logged for security monitoring. The system is designed as a hybrid model that works as a complete software-based authentication platform while also supporting future integration with IoT hardware such as Arduino or Raspberry Pi for physical door unlocking. This scalable architecture ensures flexibility for both academic implementation and real-world deployment.

The proposed system enhances security, automation, and reliability while improving user convenience through contactless authentication. It eliminates the need for physical keys, cards, or passwords and reduces the risk of unauthorized access. In addition to authentication, the system supports user management, logging, and monitoring features, making it suitable for smart homes, offices, institutions, and secure facilities. By integrating AI, machine learning, and intelligent system design, the project demonstrates the practical application of advanced technologies in modern security systems. The hybrid and scalable nature of the system makes it a strong foundation for future enhancements such as multi-factor authentication, cloud integration, and large-scale smart security infrastructure deployment.

Security and access control have become critical challenges in modern digital and physical environments due to the increasing adoption of smart infrastructure and connected systems. Traditional door locking mechanisms such as mechanical keys, password-based locks, and card-based access systems suffer from limitations including key duplication, unauthorized access, loss of credentials, and lack of intelligent authentication. These conventional systems rely heavily on physical objects or memorized information, making them vulnerable to misuse and human error. With recent advancements in Artificial Intelligence (AI), Machine Learning (ML), and Computer Vision, biometric authentication systems have emerged as a reliable and intelligent alternative. Among these, face recognition stands out as a contactless, user-friendly, and secure authentication method suitable for real-world

KEYWORDS: Face Recognition, Artificial Intelligence, Internet of Things (IoT), Smart Door Lock System, Biometric Authentication, Computer Vision, Machine Learning, Access Control System.

I. INTRODUCTION

Security and access control have become fundamental requirements in modern society due to rapid urbanization, technological growth, and the in creasing depend en ceondigital and connected systems. In every day life, peoplerely on security mechanism stop rotecthomes, offices, institutions, industries, and sensitive infrastructure. Traditionally, access control has been managed using mechanical keys, locks, passwords, access cards, and basic electronic systems. Although these methods have been widely adopted for decades, they suffer from several inherent limitations such as key duplication, unauthorized access, loss of physical keys or cards, password theft, and lack of intelligent decision-making. These traditional systems are mostly static in nature, meaning they cannot adapt or respond intelligently to changing security conditions or threats. As a result, they are increasingly becoming insufficient in meeting

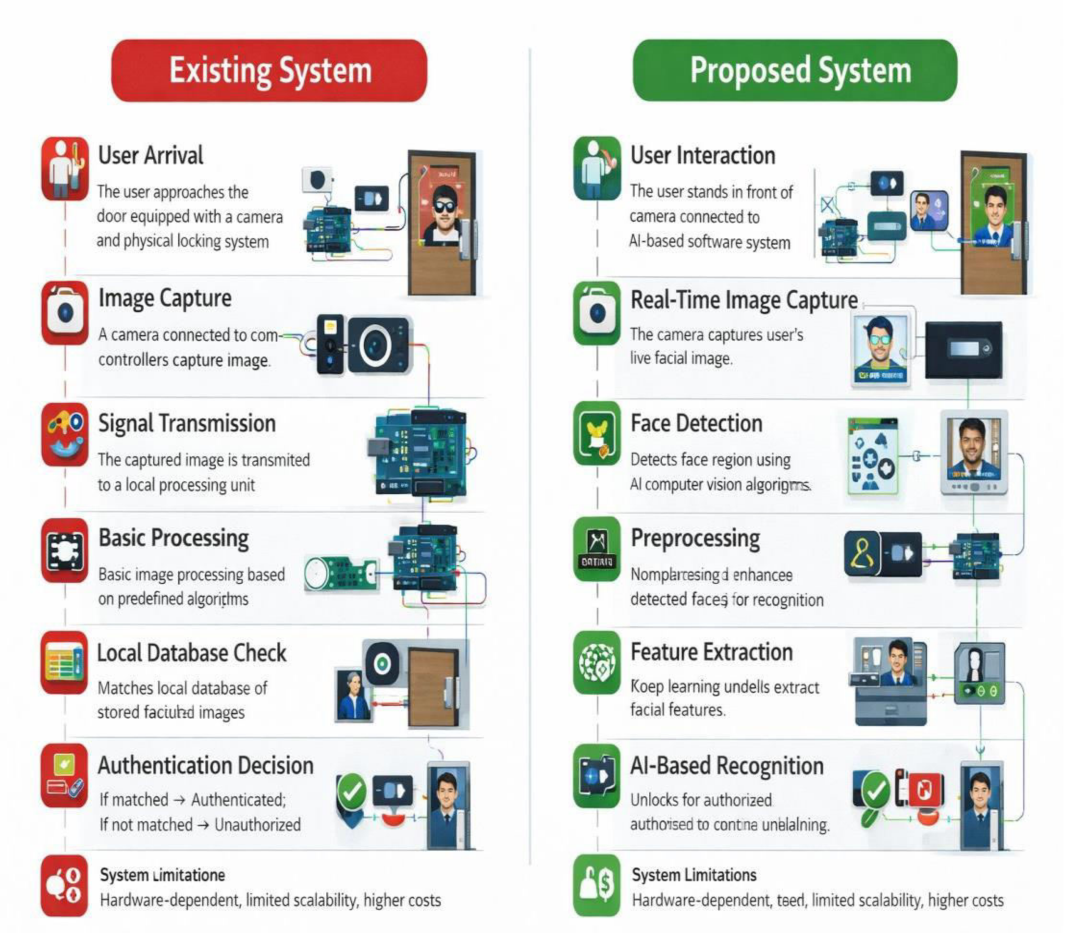
In addition to security vulnerabilities, traditional access control systems also create usability challenges. Users are required to remember multiple passwords, carry physical keys or cards, and depend on external devices for authentication. This not only increases inconvenience but also creates dependency on physical objects that can be lost, stolen, or misused. In large organizations and institutions, managing access credentials becomes a complex task, requiring manual administration, regular updates, and constant monitoring. Furthermore, conventional systems lack proper monitoring, logging, and auditing mechanisms, making it difficult to track unauthorized access attempts and security breaches.

With the rapid development of Artificial Intelligence (AI), Machine Learning (ML), and Computer Vision, new possibilities have emerged in the field of intelligent security systems. AI enables machines to learn from data, recognize patterns, and make intelligent decisions without explicit programming. Machine learning models can be trained to recognize complex patterns in images, audio, and sensor data, making them highly suitable for biometric authentication applications. Computer vision, a subfield of AI, focuses on enabling machines to interpret and understand visual information from the real world

Biometric authentication systems have gained significant importance in recent years due to their ability to identify individuals based on unique biological and behavioral characteristics. Common biometric methods include fingerprint recognition, iris scanning, voice recognition, and face recognition. Among these, face recognition has emerged as one of the most natural, contactless, and user-friendly authentication techniques. Unlike fingerprint or card-based systems, face recognition does not require physical contact or additional devices, making it more hygienic, convenient, and efficient. Users can be authenticated simply by standing infron to facamera.

II. LITERATUREREVIEW

Recent advancements in Artificial Intelligence (AI), Machine Learning (ML), and Computer Vision have significantly transformed the domain of security and access control systems. Early biometric authentication research primarily focused on fingerprint recognition, iris scanning, and voice recognition, which demonstrated improved security over traditional methods but required physical contact or specialized hardware. Laterres earch shifted toward face recognition duetoits contactless and non-intrusive nature. Initial face recognition techniques such as Eigen faces, Fisher faces, and Local Binary Patterns relied on handcrafted feature extraction methods and statistical models, achieving limited accuracy under varying lighting and environmental conditions. The emergence of deep learning, particularly Convolutional Neural Networks(CNNs), marked a major breakthrough in biometric authentication research, enabling automatic feature extraction and high-accuracy recognition. Deep learning models such as VGG Net, Res Net, Face Net, and VGG-Face laid the foundation for modern face recognition systems and demonstrated superior performance compared to traditional methods**.**


Existing System
User Arrival
The user approaches the door equipped with a camera and physical locking system
Image Capture
A camera connected to com-controllers capture image.
Signal Transmission
The captured image is transmited to a local processing unit
Basic Processing
Basic image processing based on predefined algoritms
Local Database Check
Matches local database of stored faciuhd images
Authentication Decision
If matched → Authenticated;
If not matched → Unauthorized
System Limitatione
Hardware-dependent, limited scalability, higher costs
Proposed System
User Interaction
The user stands in front of camera connected to AI-based software system
Real-Time Image Capture
The camera captures user's live facial image.
Face Detection
Detects face region using AI computer vision algorigms.
Preprocessing
Nomplarcesing d enhance detected faces for recognition
Feature Extraction
Koep learning undells extract facial features.
AI-Based Recognition
Unlocks for authorized authoised to contine unlalning.
System Limitations
Hardware-dependent, tsed, limited scalability, higher costs

2.1 Existing System

The existing smart door unlocking systems are primarily based on hardware-dependent architectures that integrate cameras, microcontrollers such as Arduino or Raspberry Pi, and physical locking mechanisms like servo motors or solenoid locks. In these systems, the user approaches the door and the camera captures the facial image, which is then transmitted to a local processing unit for basic image processing and pattern matching using predefined algorithms. The captured image is compared with a limited local database of stored facial templates to determine authentication. If a match is found, a control signal is generated to activate the physical locking mechanism and unlock the door; otherwise, access is denied. Although these systems provide basic biometric security, they are limited by fixed deployment, depend encyonphysical hardware, restrictedscalability, higher implementation and maintenance costs, and limited adaptability to en vironmental variations and large-scale deployments.

2.2 Proposed System

The proposed system is an AI-Based Smart Door Unlock System using Face Recognition, designed asan intelligent, software-driven access control platform with future IoT integration capability. The system captures real-time facial images using a camera and applies computer vision and deep learning techniques to detect faces, preprocess images, and extract unique facial features automatically. These features are compared with a trained image database of authorized users using machine learning models to perform accurate authentication and authorization. Based on the AI decision engine, the system generates an access outcome as “Access Granted” or “Access Denied,” which is displayed through the user interface and logged for monitoring and security auditing. The system is built on a hybrid and scalable architecture that functions as a complete software-based authentication solution while supporting future integration with physical locking mechanisms such as Arduino, Raspberry Pi, and IoT devices for real-world deployment, making it secure, flexible, and suitable for modern smart security environments.

III. METHODOLOGY

3.1 System Architecture Design

The system is designed using a hybrid architecture that combines artificial intelligence-based software processing with future-ready IoT integration. The architecture includes input devices (camera), AI processing modules, machine learning models, databases, user interfaces, and optional hardware integration layers. This modular design allows the system to function as a complete software-based authentication platform while supporting futurephysical deployment with smart locking mechanisms.

3.2 Data Collection and Image Database Creation

Facial images of authorized users are collected using a camera or image input interface. Multiple images per user are captured under different lighting conditions, facial expressions, and angles to improve recognition accuracy. These images are stored in a structured image database and labeled with unique user identities. This dataset acts as the training and reference dataset for the face recognition model.

3.3 Image Acquisition

The system captures real-time facial images or live video frames using a connected camera. Continuous image acquisition ensures real-time monitoring and dynamic interaction with the user during the authentication process.

3.4 Face Detection

Computer vision algorithms are used to detect the presence of a human face in the captured image. The face region is isolated from the background using detection models, ensuring that only relevant facial data is processed further.

3.5 Image Preprocessing

The detected facial image undergoes preprocessing operations such as resizing, normalization, grayscale conversion, noise reduction, and contrast enhancement. These steps improve image quality and standardize input data for accurate feature extraction and recognition

3.6 Feature Extraction

Deep learning models based on Convolutional Neural Networks (CNNs) automatically extract unique facialfeatures from the preprocessed images. These features represent the biometric identity of the user in a numerical form that can be efficiently compared and analyzed by machine learning algorithms.

3.7 Mode lTraining

The extracted facial features from the labeled dataset are used to train the machine learning model. The model learns to distinguish between different users by identifying unique patterns in facial structures. Training improves system accuracy and recognition performance over time.

3.8 Face Recognition and Authentication

During real-time operation, the system compares the extracted features of the captured face with the trained image database. Machine learning classification algorithms determine whether the face matches any authorized user profile.

3.9 Authorization Process

Once the user is authenticated, the system verifies access permissions and authorization rules such as user roles, access levels, and time-based access control policies to determine whether access should be granted.

3.10 Decision Engine

The AI decision engine generates the final output based on authentication and authorization results. The decision is classified as either Access Granted or Access Denied.

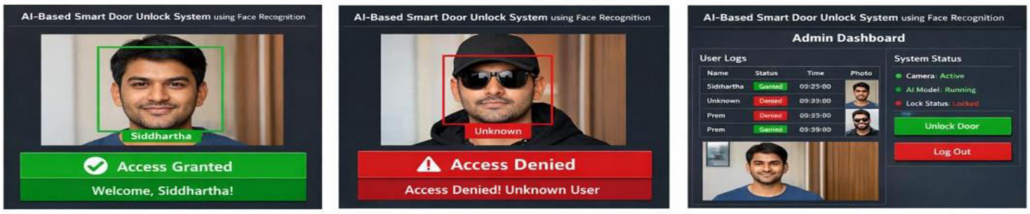
3.11 System Response and Output Display

The result of the decision engine is displayed through the user interface. The system shows authentication status, user identity (if authorized), and access messages. All access attempts are logged in the system database for monitoring and auditing.

3.12 Logging and Monitoring

Every authentication attempt is recorded with details such as user ID, timestamp, and access status. This ensures traceability, accountability, and security monitoring.

IV. IMPLEMENTATION



AI-Based Smart Door Unlock System using Face Recognition

Siddhartha

Access Granted

Welcome, Siddhartha!

AI-Based Smart Door Unlock System using Face Recognition

Unknown

Access Denied

Access Denied! Unknown User

AI-Based Smart Door Unlock System using Face Recognition

Admin Dashboard

User Logs

Name	Status	Time	Photo
Sidihartha	Ganted	09:25:00	
Unknown	Denied	09:33:00	
Prem	Denied	09:35:00	
Prem	Ganted	09:39:00	

System Status

- Camera: Active
- AI Model: Running
- Lock Status: Locked

4.1 System Setup and Environment Configuration

The implementation begins with setting up the software environment required for system development. Programming languages and frameworks such as Python, AI/ML libraries, and computer vision tools are configured. Required libraries for face detection, image processing, deep learning, and database management are installed. The system environment is prepared to support real-time image processing, machine learning model execution, and data storage operations.

4.2 Image Database Development

A structured image database is created to store facial images of authorized users. Multiple images per user are collected under different lighting conditions, facial expressions, and angles to improve recognition accuracy. Each user is assigned a unique identity, and the corresponding images are labeled and stored in the database

4.3 Camera Integration and Image Acquisition

A camera module is integrated with the system to capture real-time facial images or video frames. Continuousvideo streaming is enabled for live monitoring. The system captures frames dynamically and forwards them to the processing module for further analysis.

4.4 Face Detection Module Implementation

Face detection algorithms are implemented using computer vision techniques to identify and locate faces in the captured images. Thedetected face region isisolated from thebackground, ensuring that only relevant facial data is

4.5 Image Preprocessing Module

Preprocessing techniques such as resizing, normalization, grayscale conversion, noise reduction, and contrast enhancement are implemented to standardize the facial images. These steps improve image quality and ensure consistency of input data for machine learning models.

4.6 Feature Extraction and AI Model Integration

Deep learning models based on Convolutional Neural Networks (CNNs) are integrated into the system to extract unique facial features automatically. These features are converted into numerical representations that serve as biometric signatures for each user.

4.7 Model Training and Optimization

The AI model is trained using the labeled facial image dataset. Training involves learning facial patterns, feature correlations, and identity classification. Model optimization techniques are applied to improve accuracy, reduce false positives, and enhance recognition performance.

4.8 Real-Time Face Recognition

During system execution, real-time facial features extracted from live images are compared with the trained database using machine learning algorithms. The system identifies whether the captured face matches any authorized user profile.

4.9 Authentication and Authorization Logic

Authentication verifies user identity through face recognition, while authorization determines whether the authenticated user has permission to access the system. Role-based and rule-based authorization mechanisms are implemented to manage access control policies.

V. CONCLUSION

This project successfully presented the design and implementation of an AI-Based Smart Door Unlock System using Face Recognition, aimed at providing a secure, intelligent, and automated access control solution for modern smart environments. By integrating artificial intelligence, machine learning, and computer vision techniques, the system is capable of authenticating users in real time through facial recognition. The proposed approach eliminates the dependence on traditional security mechanisms such as physical keys, passwords, and access cards, thereby reducing.

The system demonstrates the practical application of deep learning models for biometric authentication by accurately detecting faces, extracting unique facial features, and performing reliable identity verification using a trainedimagedatabase. Thesoftware-basedimplementationprovidesacompletesmartaccesscontrolplatformwith features such as real-time authentication, user management, access logging, and system monitoring.

Overall, the proposed AI-based smart door unlock system offers an effective alternative to conventional access control systems by combining security, automation, and user convenience in a single intelligent framework. The system not only enhances security but also improves user experience through contactless authentication and intelligent decision-making. With further enhancements such as multi-factor authentication, cloud integration, and large-scale deployment, the system has the potential to evolve into a comprehensive smart security solution for next-generation smart infrastructures.

VI. FUTURE SCOPE

The AI-Based Smart Door Unlock System using Face Recognition offers significant potential for future enhancements and large-scale real-world deployment. One of the major directions for future development is the integration of physical locking mechanisms using IoT technologies such as Arduino, Raspberry Pi, relay modules, and solenoidlockstoena blereal- worldauto matic door unlocking. Thiswill transform the system from a software- based authentication platformintoafully functional smart security system suitable forhomes, offices, institutions, and industrial environments.The system can be further enhanced by implementing multi-factor authentication, combining face recognitionwith additional security layers such as One-Time Passwords (OTP), RFID cards, mobile authentication, or biometric fusion techniques. This will significantly improve security in high-risk and high-sensitivity environments such as banks, laboratories, data centers, and restricted facilities. Role-based access control, time- based access policies, and location-based authentication can also be integrated to provide fine-grained access management

REFERENCES

1. Vani, S., Malathi, P., Ramya, V. J., Sriman, B., Saravanan, M., & Srivel, R. (2024). An efficient black widow optimization-based faster R-CNN for classification of COVID-19 from CT images. Multimedia Systems, 30(2), 108.
2. Kumar, A. S., Saravanan, M., Joshna, N., & Seshadri, G. (2019). Contingency analysis of fault and minimization of power system outage using fuzzy controller. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4111-4115.
3. David, A. (2020). Air pollution control monitoring & delivery rate escalated by efficient use of markov process in manet networks: to measure quality of service parameters. Test Engineering & Management, The Mattingley Publishing Co., Inc. ISSN, 0193-4120.
4. Saravanan, M., Kumar, A. S., Devasaran, R., Seshadri, G., & Sivaganesan, S. (2019). Performance analysis of very sparse matrix converter using indirect space vector modulation. Intern. Jou. of Inn. Techn. and Expl. Eng, 9(1), 4756-4762.
5. Saravanan, M., & Sivakumaran, T. S. (2016). Three phase dual input direct matrix converter for integration of two AC sources from wind turbines. Circuits Syst., 7, 3807-3817.
6. Dharnasi, P. (2025). A Multi-Domain AI Framework for Enterprise Agility Integrating Retail Analytics with SAP Modernization and Secure Financial Intelligence. International Journal of Humanities and Information Technology, 7(4), 61-66.
7. Amitha, K., Ram Manohar Reddy, M., Yashwanth, K., Shylaja, K., Rahul Reddy, M., Srinu, B., & Dharnasi, P. (2026). AI empowered security monitoring system with the help of deployed ML models. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 69–73.
8. Gogada, S., Gopichand, K., Reddy, K. C., Keerthana, G., Nithish Kumar, M., Shivalingam, N., & Dharnasi, P. (2026). Cloud computing/deep learning customer churn prediction for SaaS platforms. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 74–78.
9. Akula, A., Budha, G., Bingi, G., Chanda, U., Borra, A. R., Yadav, D. B., & Saravanan, M. (2026). Emotion recognition from facial expressions using CNNs. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(1), 120–125.
10. Varshini, M., Chandrapathi, M., Manirekha, G., Balaraju, M., Afraz, M., Sarvanan, M., & Dharnasi, P. (2026). ATM access using card scanner and face recognition with AIML. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 113–118.
11. Feroz, A., Pranay, D., Srikar Sai Raj, B., Harsha Vardhan, C., Rohith Raja, B., Nirmala, B., & Dharnasi, P. (2026). Blockchain and machine learning combined secured voting system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 119–124.
12. Tirupalli, S. R., Munduri, S. K., Sangaraju, V., Yeruva, S. D., Saravanan, M., & Dharnasi, P. (2026). Blockchain integration with cloud storage for secure and transparent file management. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 79–86.
13. Chandu, S., Goutham, T., Badrinath, P., Prashanth Reddy, V., Yadav, D. B., & Dharnas, P. (2026). Biometric authentication using IoT devices powered by deep learning and encrypted verification. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(1), 87–92.
14. Singh, K., Amrutha Varshini, G., Karthikeya, M., Manideep, G., Sarvanan, M., & Dharnasi, P. (2026). Automatic brand logo detection using deep learning. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(1), 126–130.
15. Keerthana, L. M., Mounika, G., Abhinaya, K., Zakeer, M., Chowdary, K. M., Bhagyaraj, K., & Prasad, D. (2026). Floods and landslide prediction using machine learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 125–129.
16. Dadigari, M., Appikatla, S., Gandhala, Y., Bollu, S., Macha, K., & Saravanan, M. (2026). Bitcoin price prediction with ML through blockchain technology. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 130–136.
17. Chinthala, S., Erla, P. K., Dongari, A., Bantu, A., Chityala, S. G., & Saravanan, M. S. (2026). Food recognition and calorie estimation using machine learning. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 480–488.
18. Chinthamalla, N., Anumula, G., Banja, N., Chelluboina, L., Dangeti, S., Jitendra, A., & Saravanan, M. (2026). IoT-based vehicle tracking with accident alert system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 486–494.

19. Nagamani, K., Laxmikala, K., Sreeram, K., Eshwar, K., Jitendra, A., & Dharnasi, P. (2026). Disaster management and earthquake prediction system using machine learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 495–499.
20. Prasad, E. D., Sahithi, B., Jyoshnavi, C., Swathi, D., Arun Kumar, T., Dharnasi, P., & Saravanan, M. (2026). A technology driven – solution for food and hunger management. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 440–448.
21. Rakesh, V., Vinay Kumar, M., Bharath Patel, P., Varun Raj, B., Saravanan, M., & Dharnasi, P. (2026). IoT-based gas leakage detector with SMS alert. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 449–456.
22. Chanamalla, B., Murali, V. N., Suresh, B., Deepak, M. S., Zakriya, M., Yadav, D. B., & Saravanan, M. (2026). AI-driven multi-agent shopping system through e-commerce system. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 463–470.
23. Bhagyasri, Y., Bhargavi, P., Akshaya, T., Pavansai, S., Dharnasi, P., & Jitendra, A. (2026). IoT based security & smart home intrusion prevention system. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 457–462.
24. Thotla, S. B., Vyshnavi, S., Anusha, P., Vinisha, R., Mahesh, S., Yadav, D. B., & Dharnasi, P. (2026). Traffic congestion prediction using real time data by using deep learning techniques. , 8(2), 489–494.
25. Rupika, M., Nandini, G., Mythri, M., Vasu, K., Abhiram, M., Shivalingam, N., & Dharnasi, P. (2026). Electronic gadget addiction prediction using machine learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 500–505.
26. Akshaya, N., Balaji, Y., Chennarao, J., Sathwik, P., & Dharnasi, P. (2026). Diabetic retinopathy diagnosis with deep learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 506–512.
27. Pavan Kumar, T., Abhishek Goud, T., Yogesh, S., Manikanta, V., Dinesh, P., Srinu, B., & Dharnasi, P. (2026). Smart attendance system using facial recognition for staff using AI/ML. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 513–519. https://doi.org/10.15662/IJRPETM.2026.0902005
28. Reddy, V. N., Rao, P. H. S., Singh, N. S., Kumar, V. S. S., Reddy, Y. B., & Dharnasi, P. (2026). Face recognition using criminal identification system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 520–527.
29. Rachana, P., Kalyan, P. P., Kumar, T. S., Reddy, P. M., Rohan, P., Saravanan, M., & Dharnasi, P. (2026). Secure chat application with end-to-end encryption using deep learning. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 472–478.
30. Krishna, G., Rajesh, B., Dinesh, B., Sravani, B., Rajesh, G., Dharnasi, P., & Sarvanan, M. (2026). Smart agriculture system using IoT with help of AI-techniques. International Journal of Computer Technology and Electronics Communication, 9(2), 479–487.
31. Reddy, N. H. V., Reddy, N. T., Bharath, M., Hemanth, N., Dharnasi, D. P., Nirmala, B., & Jitendra, A. (2026). AI based learning assistant using machine learning. International Journal of Engineering & Extended Technologies Research, 8(2), 495–504.
32. Vangara, N., Bhargavi, P., Chandu, R., Bhavani, V., Yadav, D. B., & Dharnasi, P. (2026). Machine learning based intrusion detection system using supervised and unsupervised learning. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 505–511.
33. Yadamakanti, S., Mahesh, Y., Rathnam, S. A., Praveen, V., Jitendra, A., & Dharnasi, P. (2026). Unified Payments Interface fraud detection using machine learning. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 488–497.
34. Basha, S. A., Krishna, V. S. B., Shanker, S. S., Sravya, R., Shivalingam, N., & Dharnasi, P. (2026). AI-powered price prediction for agriculture markets. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 512–515.
35. Sanjay, P., Vardhan, Y. H., Raja, S. Y., Krishna, V. M., Nirmala, B., & Dharnasi, P. (2026). Disaster management and earthquake tsunami prediction system using machine learning and deep learning. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 516–522.
36. Varsha, P., Chary, P. K., Sathvik, P., Varma, N. V., Rahul, S., Saravanam, M., & Dharnasi, P. (2026). IoT-based fire alarm and location tracking system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 528–532.
37. Priya, B. A., Gayathri, D., Maheshwari, B., Nikhitha, C., Sravanam, D., Yadav, D. B., & Saravanan, M. (2026). Fake news detection using natural language processing. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 498–505.

DOI: 10.15680/IJCTECE.2026.0902011

38. Swathi, B., Aravind, A., Sharath Chandra, A., Sunethra, B., Bhanu Reddy, C., Jitendra, A., & Sarvanan, M. (2026). Deep learning enable smart trafficking management system. *International Journal of Research Publications in Engineering, Technology and Management, 9*(2), 533–539.
39. Peravali, S., Yelighti, H. V., Shaganti, Y. R., Velamati, M. K., Nirmala, B., Saravanan, M., & Dharnasi, P. (2026). Disaster management and earthquake/tsunami prediction system using machine learning and deep learning. *International Journal of Research Publications in Engineering, Technology and Management, 9*(2), 540–548.
40. Prasad, M. H. A., Goutham, G., Nithish, J., Hardhik, G., Rahman, M. A., Saravanan, M., & Dharnasi, P. (2026). Deepfake face detection using machine learning. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, **8**(2), 523–548.