Alert System Using Facial Recognition

I.Karthika Varsha[1], K.Madhu Krishna[2], P.Saishma[3], Mrs.E.Harika[4]

[1,2,3,4]*Department of Computer Science and Engineering, Anurag University, India.*

Corresponding author's email: *geethasrinivas1010@gmail.com*
madhukrishna2419@gmail.com
pittalasaishma654@gmail.com

Abstract. This research work presents a cost-effective facial recognition alert system using the ESP32 microcontroller to enhance real-time security. The system integrates high-resolution cameras with Python's facial recognition libraries to identify individuals. When an unknown face is detected, it triggers an immediate alert via the ESP32, activating an alarm. This solution is both scalable and affordable, making advanced security accessible to small businesses and residential areas. The system improves overall security by automating surveillance, reducing the need for manual monitoring**.**

Keywords. Facial Recognition, Real-Time Monitoring, ESP32 Microcontroller, Security System, Alert System, Automated Surveillance, Unauthorized Detection

1. INTRODUCTION

Facial recognition technology is becoming a key part of modern security systems, allowing for automatic identification and monitoring of people. Traditional security methods like ID cards or passwords are being replaced by biometric systems, which are more reliable and efficient. However, many facial recognition systems are expensive and complicated to set up, which makes them difficult to use for small businesses or personal security. To solve this problem, our project focuses on building an affordable facial recognition alert system using the low-cost ESP32 micro controller.

The system is designed to automatically identify authorized people and detect intruders in real time. By using cameras and facial recognition software, it continuously monitors important areas and triggers an alert when an unknown face is detected. The ESP32 micro controller makes the system affordable and ensures fast alerts without needing to rely on the internet, making it a practical and accessible security solution for homes, offices, and small businesses.

2. RESEARCH METHODOLOGY

The research methodology for the Facial Recognition Alert System involves several key stages: system design, hardware and software selection, implementation, and testing. This section outlines the approach taken to develop an affordable, real-time facial recognition system for security purposes.

2.1 System Design

The system is designed to detect and recognize faces in real-time and trigger an alert if an unknown individual is identified. The major components include a camera for video input, a facial recognition algorithm for processing, and the ESP32 microcontroller for triggering alerts. The overall system architecture ensures real-time detection with minimal latency.

2.2 Hardware Selection

The hardware components selected for the project include:

Camera: High-definition cameras to capture video feeds and detect faces.

ESP32 Microcontroller: Chosen for its cost-effectiveness and ability to connect to Wi-Fi for real-time alerting. The ESP32 microcontroller was selected due to its low cost, power efficiency, and ability to handle WebSocket communication for triggering alarms.

3 SOFTWARE DEVELOPMENT

The system is developed using the following software tools:

Python: Python was chosen as the primary programming language due to its powerful libraries for image processing and facial recognition.

OpenCV: Used for detecting and capturing faces from the video feed.

Face Recognition Library: The face_recognition library is used to compare detected faces with a database of authorized personnel.

WebSocket Protocol: A WebSocket client library is integrated to enable real-time communication between the recognition system and the ESP32 microcontroller.

Arduino IDE: Used to program the ESP32 microcontroller for controlling the alert system (buzzer).

4. IMPLEMENTATION

The system follows a multi-step implementation process:

Face Detection: The camera continuously captures video, and OpenCV detects faces within the video frame.

Face Recognition: Detected faces are compared against a pre-loaded database of authorized individuals using the face_recognition library. If the face matches an entry in the database, no action is taken. If it does not match, the system considers the individual as "unknown."

Alert Mechanism: Upon detecting an unknown face, the system sends a signal to the ESP32 microcontroller via WebSocket. The ESP32 triggers a connected buzzer or sends an alert to the security personnel.

5. TESTING AND EVALUATION

The system is tested in various real-world conditions, including different lighting environments and angles of face detection, to evaluate its performance. The accuracy of face recognition is measured by comparing the number of correct identifications versus false positives/negatives. The efficiency of the alert system is tested by timing how quickly the ESP32 triggers the alarm after detecting an unknown face. Additionally, the system's scalability is tested by integrating multiple cameras to cover a wider area.

6. ETHICAL AND PRIVACY CONSIDERATIONS

Ethical concerns surrounding the use of facial recognition technology were considered. The system is designed to comply with data protection and privacy laws by ensuring that all facial data is stored securely and is accessible only by authorized users. Users are also informed about the ethical use of facial recognition in monitoring and surveillance environments.

6.1 Results

An easy-to-use, lightweight alert system was developed using facial recognition technology. This system was tested for a variety of security-related tasks, including identification of authorized personnel and alerting for unknown individuals at various access points. The system accurately identified more than 95% of pre-defined authorized individuals in real-time, based on an initial training phase where images of known persons were provided to the system. The alert mechanism, triggered by the ESP32 microcontroller, successfully activated alarms or notifications when an unauthorized face was detected.

One of the major success factors was the system's flexibility in recognizing faces under various conditions, such as different lighting environments or angles, which made it highly effective for non-experts in security management. The real-time alerting system ensured that security personnel were notified within 2 seconds, enhancing response time significantly. Additionally, the system is able to scale and handle multiple camera feeds, making it suitable for large-scale security setups like offices or residential buildings. The system also demonstrated cost-effectiveness, making advanced facial recognition accessible to users with limited budgets, which is a key achievement of the project.

6.2 Discussion

The facial recognition-based alert system offers significant flexibility compared to traditional security methods, which often rely on manual monitoring or static authentication techniques like access cards. By employing AI-powered real-time facial recognition, this system automatically identifies authorized individuals and triggers alerts for unknown faces, enhancing security in sensitive areas. The integration of the ESP32 microcontroller ensures a cost-effective solution that maintains low latency and rapid response times, making it suitable for a variety of environments, from residential settings to restricted access zones.

While the system demonstrated a high accuracy rate in identifying known individuals, there are opportunities for further enhancement, particularly in challenging conditions such as low lighting. Improving its performance in these scenarios and expanding the database of recognized faces will increase its effectiveness and versatility. As security needs continue to evolve, future developments will focus on refining the system's capabilities, ensuring it remains relevant and effective in dynamic environments where unauthorized access is a concern.

Overall, this system addresses a crucial need for affordable and efficient real-time security solutions. Its adaptability and ease of use position it as a valuable tool for modern security challenges. By continuously enhancing its performance and integrating with additional security technologies, the system can provide comprehensive protection, ensuring a safer environment for users.

Preparation of Tables

TABLE 1. Performance Evaluation of the Facial Recognition System Under Different Operational Conditions

Operational Condition	Description	Accuracy (%)	Response Time (s)	Alert Success Rate (%)	System Load (%)	Comments
Indoor, Bright Light	Testing in well-lit indoor areas	**95**	**1.2**	**98**	**30**	Optimal performance, minimal delays.
Indoor, Low Light	Testing in dimly lit areas	**85**	**1.5**	**98**	**30**	Some recognition challenges, but acceptable.
Outdoor, Daylight	Testing in natural daylight	**90**	**1.3**	**95**	**35**	Good performance; however, glare can affect results
Outdoor, Night	Testing with artificial lighting	**80**	**2.0**	**85**	**50**	Reduced accuracy; infrared lighting recommended.

7. CONCLUSIONS

The Facial Recognition-Based Alert System provides an efficient, real-time security solution by combining AI-powered facial recognition with the affordable ESP8266 microcontroller for triggering alerts. It successfully identifies authorized individuals and triggers an alert when unauthorized faces are detected, offering a cost-effective way to secure sensitive areas like homes and offices. The system is scalable and performs well under most conditions, though improvements can be made for low-light environments. Overall, this project delivers a practical, accessible security solution that enhances monitoring capabilities while remaining budget-friendly.

7.1 Study Limitations

Integration Issues: Delays in communication between the facial recognition module and the ESP8266 can lead to slow alerts or missed detections, impacting system performance.

AI Limitations: The facial recognition algorithm may struggle in poor lighting or with partial obstructions, reducing accuracy and reliability.

·Data Accuracy: The system's effectiveness depends on the quality and diversity of the training dataset, with outdated data potentially leading to misidentifications.

7.2 Competing Interests

The Facial Recognition-Based Alert System asserts that there are no actual or potential conflicts of interest that could affect its development, deployment, or operation.

All data sources, algorithms, and functionalities used within the system adhere to objective security standards and rely on publicly available information. There are no commercial or financial relationships, sponsorships, or external affiliations influencing its design or performance.

REFERENCES

1. Kumar, T. V. (2018). Project Risk Management System Development Based on Industry 4.0 Technology and its Practical Implications.
2. Tambi, V. K., & Singh, N. (2015). Potential Evaluation of REST Web Service Descriptions for Graph-Based Service Discovery with a Hypermedia Focus.
3. Kumar, T. V. (2024). A Comparison of SQL and NO-SQL Database Management Systems for Unstructured Data.
4. Kumar, T. V. (2024). A Comprehensive Empirical Study Determining Practitioners' Views on Docker Development Difficulties: Stack Overflow Analysis.
5. Kumar, T. V. (2024). Developments and Uses of Generative Artificial Intelligence and Present Experimental Data on the Impact on Productivity Applying Artificial Intelligence that is Generative.
6. Kumar, T. V. (2024). A New Framework and Performance Assessment Method for Distributed Deep Neural NetworkBased Middleware for Cyberattack Detection in the Smart IoT Ecosystem.
7. Sharma, S., & Dutta, N. (2016). Analysing Anomaly Process Detection using Classification Methods and Negative Selection Algorithms.
8. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.
9. Sakshi, S. (2023). Development of a Project Risk Management System based on Industry 4.0 Technology and its Practical Implications.
10. Arora, P., & Bhardwaj, S. Mitigating the Security Issues and Challenges in the Internet of Things (IOT) Framework for Enhanced Security.
11. Sakshi, S. (2024). A Large-Scale Empirical Study Identifying Practitioners' Perspectives on Challenges in Docker Development: Analysis using Stack Overflow.
12. Sakshi, S. (2023). Advancements and Applications of Generative Artificial Intelligence and show the Experimental Evidence on the Productivity Effects using Generative Artificial Intelligence.
13. Sakshi, S. (2023). Assessment of Web Services based on SOAP and REST Principles using Different Metrics for Mobile Environment and Multimedia Conference.
14. Sakshi, S. (2022). Design and Implementation of a Pattern-based J2EE Application Development Environment.
15. Sharma, S., & Dutta, N. (2018). Development of New Smart City Applications using Blockchain Technology and Cybersecurity Utilisation. Development, 7(11).
16. Sharma, S., & Dutta, N. (2017). Development of Attractive Protection through Cyberattack Moderation and Traffic Impact Analysis for Connected Automated Vehicles. Development, 4(2).
17. Sharma, S., & Dutta, N. (2015). Evaluation of REST Web Service Descriptions for Graph-based Service Discovery with a Hypermedia Focus. Evaluation, 2(5).

18. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.
19. Sharma, S., & Dutta, N. (2015). Cybersecurity Vulnerability Management using Novel Artificial Intelligence and Machine Learning Techniques. Sakshi, S. (2023). Development of a Project Risk Management System based on Industry 4.0 Technology and its Practical Implications.
20. Sharma, S., & Dutta, N. (2017). Classification and Feature Extraction in Artificial Intelligence-based Threat Detection using Analysing Methods.
21. Sharma, S., & Dutta, N. (2016). Analysing Anomaly Process Detection using Classification Methods and Negative Selection Algorithms.
22. Sharma, S., & Dutta, N. (2015). Distributed DNN-based Middleware for Cyberattack Detection in the Smart IOT Ecosystem: A Novel Framework and Performance Evaluation Technique.
23. Bhat, S. (2015). Technology for Chemical Industry Mixing and Processing. Technology, 2(2).
24. Bhat, S. (2024). Building Thermal Comforts with Various HVAC Systems and Optimum Conditions.
25. Bhat, S. (2020). Enhancing Data Centre Energy Efficiency with Modelling and Optimisation of End-To-End Cooling.
26. Bhat, S. (2016). Improving Data Centre Energy Efficiency with End-To-End Cooling Modelling and Optimisation.
27. Bhat, S. (2015). Deep Reinforcement Learning for Energy-Saving Thermal Comfort Management in Intelligent Structures.
28. Bhat, S. (2015). Design and Function of a Gas Turbine Range Extender for Hybrid Vehicles.
29. Bhat, S. (2023). Discovering the Attractiveness of Hydrogen-Fuelled Gas Turbines in Future Energy Systems.
30. Bhat, S. (2019). Data Centre Cooling Technology's Effect on Turbo-Mode Efficiency.
31. Bhat, S. (2018). The Impact of Data Centre Cooling Technology on Turbo-Mode Efficiency.
32. Archana, B., & Sreedaran, S. (2023). Synthesis, characterization, DNA binding and cleavage studies, in-vitro antimicrobial, cytotoxicity assay of new manganese (III) complexes of N-functionalized macrocyclic cyclam based Schiff base ligands. Polyhedron, 231, 116269.
33. Archana, B., & Sreedaran, S. (2022). New cyclam based Zn (II) complexes: effect of flexibility and para substitution on DNA binding, in vitro cytotoxic studies and antimicrobial activities. Journal of Chemical Sciences, 134(4), 102.
34. Archana, B., & Sreedaran, S. (2021). POTENTIALLY ACTIVE TRANSITION METAL COMPLEXES SYNTHESIZED AS SELECTIVE DNA BINDING AND ANTIMICROBIAL AGENTS. European Journal of Molecular and Clinical Medicine, 8(1), 1962-1971.
35. Rasappan, A. S., Palanisamy, R., Thangamuthu, V., Dharmalingam, V. P., Natarajan, M., Archana, B., ... & Kim, J. (2024). Battery-type WS2 decorated WO3 nanorods for high-performance supercapacitors. Materials Letters, 357, 135640.
36. Arora, P., & Bhardwaj, S. (2017). Investigation and Evaluation of Strategic Approaches Critically before Approving Cloud Computing Service Frameworks.
37. Arora, P., & Bhardwaj, S. (2017). Enhancing Security using Knowledge Discovery and Data Mining Methods in Cloud Computing.
38. Arora, P., & Bhardwaj, S. (2017). Combining Internet of Things and Wireless Sensor Networks: A Security-based and Hierarchical Approach.
39. Arora, P., & Bhardwaj, S. (2019). Safe and Dependable Intrusion Detection Method Designs Created with Artificial Intelligence Techniques. machine learning, 8(7).
40. Arora, P., & Bhardwaj, S. (2017). A Very Safe and Effective Way to Protect Privacy in Cloud Data Storage Configurations.
41. Arora, P., & Bhardwaj, S. (2019). The Suitability of Different Cybersecurity Services to Stop Smart Home Attacks.
42. Arora, P., & Bhardwaj, S. (2020). Research on Cybersecurity Issues and Solutions for Intelligent Transportation Systems.
43. Arora, P., & Bhardwaj, S. (2021). Methods for Threat and Risk Assessment and Mitigation to Improve Security in the Automotive Sector. Methods, 8(2).
44. Onyema, E. M., Gude, V., Bhatt, A., Aggarwal, A., Kumar, S., Benson-Emenike, M. E., & Nwobodo, L. O. (2023). Smart Job Scheduling Model for Cloud Computing Network Application. *SN Computer Science*, *5*(1), 39.
45. Hasnain, M., Gude, V., Edeh, M. O., Masood, F., Khan, W. U., Imad, M., & Fidelia, N. O. (2024). Cloud-Enhanced Machine Learning for Handwritten Character Recognition in Dementia Patients. In *Driving Transformative Technology Trends With Cloud Computing* (pp. 328-341). IGI Global.
46. Kumar, M. A., Onyema, E. M., Sundaravadivazhagan, B., Gupta, M., Shankar, A., Gude, V., &

Yamsani, N. (2024). Detection and mitigation of few control plane attacks in software defined network environments using deep learning algorithm. *Concurrency and Computation: Practice and Experience*, *36*(26), e8256.

47. Gude, V., Lavanya, D., Hameeda, S., Rao, G. S., & Nidhya, M. S. (2023, December). Activation of Sleep and Active Node in Wireless Sensor Networks using Fuzzy Logic Routing Table. In *2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 1358-1360). IEEE.
48. Gorantla, V. A. K., Sriramulugari, S. K., Gorantla, B., Yuvaraj, N., & Singh, K. (2024, March). Optimizing performance of cloud computing management algorithm for high-traffic networks. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 482-487). IEEE.
49. Sriramulugari, S. K., & Gorantla, V. A. K. (2023). Deep learning based convolutional geometric group network for alzheimer disease prediction. *International Journal of Biotech Trends and Technology*, *13*(3).
50. Sriramulugari, S. K., & Gorantla, V. A. K. Cyber Security using Cryptographic Algorithms.
51. Gorantla, V. A. K., Sriramulugari, S. K., Mewada, A. H., Jiwani, N., & Kiruthiga, T. (2023, December). The slicing based spreading analysis for melanoma prediction using reinforcement learning model. In *2023 IEEE Technology & Engineering Management Conference-Asia Pacific (TEMSCON-ASPAC)* (pp. 1-7). IEEE.
52. Sriramulugari, S. K., Gorantla, V. A. K., Mewada, A. H., Gupta, K., & Kiruthiga, T. (2023, December). The opinion based analysis for stressed adults using sentimental mining model. In *2023 IEEE Technology & Engineering Management Conference-Asia Pacific (TEMSCON-ASPAC)* (pp. 1-6). IEEE.
53. Gorantla, V. A. K., Sriramulugari, S. K., Mewada, A. H., Gupta, K., & Kiruthiga, T. (2023, December). The smart computation of multi-organ spreading analysis of COVID-19 using fuzzy based logical controller. In *2023 IEEE Technology & Engineering Management Conference-Asia Pacific (TEMSCON-ASPAC)* (pp. 1-7). IEEE.
54. Gude, Venkataramaiah (2023). Machine Learning for Characterization and Analysis of Microstructure and Spectral Data of Materials. *International Journal of Intelligent Systems and Applications in Engineering* 12 (21):820 - 826.
55. Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., ... & Adigo, A. G. (2022). Machine Learning-Based Secure Data Acquisition for Fake Accounts Detection in Future Mobile Communication Networks. *Wireless Communications and Mobile Computing*, *2022*(1), 6356152.
56. Kalaiselvi, B., & Thangamani, M. (2020). An efficient Pearson correlation based improved random forest classification for protein structure prediction techniques. *Measurement*, *162*, 107885.
57. Thangamani, M., Satheesh, S., Lingisetty, R., Rajendran, S., & Shivahare, B. D. (2025). Mathematical Model for Swarm Optimization in Multimodal Biomedical Images. In *Swarm Optimization for Biomedical Applications* (pp. 86-107). CRC Press.
58. Chithrakumar, T., Mathivanan, S. K., Thangamani, M., Balusamy, B., Gite, S., & Deshpande, N. (2024, August). Revolutionizing Agriculture through Cyber Physical Systems: The Role of Robotics in Smart Farming. In *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)* (Vol. 1, pp. 1-6). IEEE.
59. Tiwari, V., Ananthakumaran, S., Shree, M. R., Thangamani, M., Pushpavalli, M., & Patil, S. B. (2024). RETRACTED ARTICLE: Data analysis algorithm for internet of things based on federated learning with optical technology. *Optical and Quantum Electronics*, *56*(4), 572.
60. Sakthivel, M., SivaSubramanian, S., Prasad, G. N. R., & Thangamani, M. (2023). Automated detection of cardiac arrest in human beings using auto encoders. Measurement: Sensors, 27, 100792.
61. CHITHRAKUMAR, T., THANGAMANI, M., KSHIRSAGAR, R. P., & JAGANNADHAM, D. (2023). MICROCLIMATE PREDICTION USING INTERNET OF THINGS (IOT) BASED ENSEMBLE MODEL. *Journal of Environmental Protection and Ecology*, *24*(2), 622-631.
62. Vasista, T. G. K. (2017). Towards innovative methods of construction cost management and control. *Civ Eng Urban Plan: Int J*, *4*, 15-24.
63. Hsu, H. Y., Hwang, M. H., & Chiu, Y. S. P. (2021). Development of a strategic framework for sustainable supply chain management. *AIMS Environmental Science*, (6).
64. Venkateswarlu, M., & Vasista, T. G. (2023). Extraction, Transformation and Loading Process in the Cloud computing scenario. *International Journal of Engineering Applied Sciences and Technology*, *8*, 232-236.
65. Sagar, M., & Vanmathi, C. (2022, August). Network Cluster Reliability with Enhanced Security and Privacy of IoT Data for Anomaly Detection Using a Deep Learning Model. In *2022 Third*

International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT) (pp. 1670-1677). IEEE.

66. Sagar, M., & Vanmathi, C. (2024). A Comprehensive Review on Deep Learning Techniques on Cyber Attacks on Cyber Physical Systems. *SN Computer Science*, *5*(7), 891.
67. Sagar, M., & Vanmathi, C. (2024). Hybrid intelligent technique for intrusion detection in cyber physical systems with improved feature set. *Journal of Intelligent & Fuzzy Systems*, (Preprint), 1-17.
68. Vanmathi, C., Mangayarkarasi, R., Prabhavathy, P., Hemalatha, S., & Sagar, M. (2023). A Study of Human Interaction Emotional Intelligence in Healthcare Applications. In *Multidisciplinary Applications of Deep Learning-Based Artificial Emotional Intelligence* (pp. 151-165). IGI Global.
69. Kumar, N. A., & Kumar, J. (2009). *A Study on Measurement and Classification of TwitterAccounts*.
70. Senthilkumar, S., Haidari, M., Devi, G., Britto, A. S. F., Gorthi, R., & Sivaramkrishnan, M. (2022, October). Wireless bidirectional power transfer for E-vehicle charging system. In *2022 International Conference on Edge Computing and Applications (ICECAA)* (pp. 705-710). IEEE.
71. Firos, A., Prakash, N., Gorthi, R., Soni, M., Kumar, S., & Balaraju, V. (2023, February). Fault detection in power transmission lines using AI model. In *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1-6). IEEE.
72. Gorthi, R. S., Babu, K. G., & Prasad, D. S. S. (2014). Simulink model for cost-effective analysis of hybrid system. *International Journal of Modern Engineering Research (IJMER)*, *4*(2).
73. Rao, P. R., & Sucharita, D. V. (2019). A framework to automate cloud based service attacks detection and prevention. *International Journal of Advanced Computer Science and Applications*, *10*(2), 241-250.
74. Rao, P. R., Sridhar, S. V., & RamaKrishna, V. (2013). An Optimistic Approach for Query Construction and Execution in Cloud Computing Environment. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5).
75. Rao, P. R., & Sucharita, V. (2020). A secure cloud service deployment framework for DevOps. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(2), 874-885.
76. Selvan, M. A., & Amali, S. M. J. (2024). RAINFALL DETECTION USING DEEP LEARNING TECHNIQUE.