International Journal of Data Informatics and Intelligent Computing (IJDIIC)
Vol. 4, No. 3, September 2025, pp. 14~22
DOI: 10.59461/ijdiic.v4i3.208

A Real-Time Smart Door Access Control System Using Haar Cascade Classifier and Embedded Vision

Chukwuemeka Obasi[1], Kasim Mohammed Tahir[1]
[1]Department of Computer Engineering, Edo State University Iyamho, Nigeria

Article Info

Article history:

Received May 08, 2025
Revised July 20, 2025
Accepted July 29, 2025

Keywords:

Facial Recognition
Smart Door Lock
Haar Cascade Algorithm
Embedded Vision
ESP32-CAM
IoT Security System
Real-Time Access Control

ABSTRACT

Traditional access control methods, such as mechanical keys and PIN-based systems, are ever more vulnerable to theft, copying, and unauthorized access, while high-fidelity biometric systems require intensive computing resources not suitable for low-power embedded systems. This research addresses the difficulty of achieving a real-time contactless face recognition system that compromises between security, performance, and expense in the resource-constrained embedded IoT setting. We show the design and test of an intelligent door access system using a Haar Cascade classifier on the ESP32-CAM module with cloud analytics for enhanced control, monitoring, and data logging. The system is developed to perform well on resource-constrained hardware while providing secure and remote access control. Experimental trials under varying light conditions, facial angles, and image resolutions show that the system detects faces with 97% accuracy, with a mean detection time of 151.25 milliseconds and CPU utilization of 40.5%. By adapting conventional machine learning for embedded vision, this project bridges the gap between high-fidelity biometric security and real-world IoT deployment in practice, offering an affordable and scalable solution for office and home access control in contemporary times.

Corresponding Author: Chukwuemeka Obasi (e-mail: chukwuemeka.obasi@edouniversity.edu.ng)

1. INTRODUCTION

Security is an important aspect of modern life. Access control is a common and easy security system in many homes. The development of security systems has undergone several advancements in recent times, which have moved from mechanical locks to biometric systems. Keys and keycards that were once the standard for entry control can not be fully trusted since they can be duplicated, misplaced, and stolen [1]. Biometric verification, and face recognition in particular, offers a better secure option through the use of irreversible physiological traits difficult to replicate [2]. In recent times, facial recognition technology has gained a lot of improved accuracy and performance and is a favourite in today's access control systems [3]. This is a result of the advances in artificial intelligence (AI) and deep learning. An interesting benefit of facial recognition is that it is contactless as opposed to fingerprinting or iris scanning, operating without contact, thus contributing to hygiene and convenience [4], [5] and thus displacing the need for physical keys or cards [6].

Moreover, the merging of facial recognition with the Internet of Things (IoT) has transformed security systems by making internet-connected and communicable smart door locks [7]. The monitoring of remote tasks with real-time notification and simple control actions using mobile devices is achievable using this approach, making the system easily applicable in smart homes and business environments [8], although this will not be without some challenges that need to be addressed urgently.

The Haar Cascade classifier is the most commonly used algorithm for facial recognition in access control systems, as proposed by Viola and Jones. The algorithm is highly efficient in terms of speed and real-time face detection, and therefore is highly suitable for embedded vision systems as well as low-power systems. The Haar Cascade sweeps an image at various scales using a series of simple rectangular features, quickly eliminating areas not likely to contain a face and focusing processing where most necessary.

Its use in security systems has enabled fast face localization before more profound recognition processes can be carried out. Despite the emergence of deep learning methods, Haar Cascades remain applicable in low-weight applications due to their quasi-zero computational complexity and proven performance in constrained settings [9].

This research attempts to close the gap in achieving a real-time hand-free face recognition system that provides security, performance, and cost in a resource-constrained embedded system. It presents a facial recognition technology-based smart door lock system that uses IoT to conveniently provide security access control to homes. The system focuses on contactless security access control that reduces latency and improves the efficiency of facial recognition in an IoT environment while providing security access control remotely.

2. LITERATURE REVIEW

Mechanical lock systems dominated the domain of access control systems in the early days. The recent era of lock systems uses sophisticated biometric technology. Early security devices employed physical security methods such as keys, PIN codes, and keycards. While these offered some level of protection, they were also fault-prone in the form of susceptibility to loss, copying, and theft [10]. Lock-picking and tampering have been the major bane of the Traditional lock system, which compromises the system and thereby leads to unauthorized access. These technologies were not immune to security vulnerabilities, such as password sharing, lost cards, and hacking [11]. The vulnerabilities of these traditional systems paved the way for the implementation of biometric security systems, which offer stronger authentication through the use of unique biological features that are difficult to replicate.

The emergence of biometric identification systems birthed an era of security access control with secure and reliable features, offering identity authentication based on unique physiological or behavioural characteristics. Fingerprint scanning, iris scanning, and facial recognition are the most popular among the biometric technologies due to their high accuracy and security [12]. Fingerprint verification, though standard, is contact-based and thus presents hygiene concerns, especially in public settings [4]. Iris scanning is highly precise but user-specific, hardware-dependent, and hence less convenient for regular use [12]. Facial recognition, as a contactless or remote application, among many other technologies, has gained acceptance, and also offers a non-intrusive advantage. With image processing algorithms using AI, facial recognition can authenticate people rapidly, and therefore is suitable for security applications such as airports, smart houses, and offices [13]. Facial recognition systems offer simple access control without requiring the users to come in physical contact with a device, unlike conventional authentication systems.

Recent advances in artificial intelligence (AI) and deep learning have transformed facial recognition systems, particularly in security. Traditional AI-based face detection approaches, such as Haar cascades, were feature-based, and pre-trained classifier approaches were employed to locate facial structures [14]. Traditionally, the approach was effective in earlier applications; however, it lacks flexibility and precision in challenging situations. The introduction of deep learning models, specifically convolutional neural networks (CNNs), has improved the accuracy of face recognition by enabling systems to learn and extract more complicated and discriminative face patterns [13]. For example, FaceNet, introduced by [15], revolutionized face recognition by developing strong face embeddings that significantly improved speed and accuracy. Elaborating further, [16] and [17] demonstrated how the integration of CNNs and recurrent neural networks (RNNs) would enable real-time face recognition for smart door lock systems. These powerful models are, nevertheless, computationally intensive, which becomes a concern if they are to be deployed on low-power and resource-constrained IoT devices that are typically used in home automation.

In order to overcome this trade-off between performance and computational cost, [18] developed a system using the YOLO algorithm on a board of Jetson Nano. The configuration achieved 99% high accuracy and a mean recognition time of 0.6 seconds in bright conditions. Similarly, [19] employed Eigenface and Principal Component Analysis (PCA) on a Raspberry Pi with 90% accuracy and 15-second recognition time—a huge improvement from the more than 30 seconds latency that [20] experienced in an ESP32-CAM and Android-based smart lock system. More integrated in their methodology was [21], who used a CNN-based deep model on a Raspberry Pi 3 for home security. Although their system allowed remote monitoring for real-time access control, no performance measure was reported. However, with the implementation of deep learning on a limited platform, hardware optimization would clearly be necessary in order to speed up recognition as well as increase accuracy.

In the aspect of system integration, [22] designed a remote real-time monitoring system with facilities of notifications, alarms, and limited facial recognition features. However, the lack of full user-specific biometric verification posed issues in cybersecurity since it left the system vulnerable to unwanted access.

The integration of facial recognition-based security with a healthcare monitoring system is very helpful in times of public health emergencies such as the COVID-19 pandemic. Presented [23] an integrated

system using facial recognition with contactless body temperature measurement achieved with the deployment of Raspberry Pi 3B+, OpenCV, and the MLX90614 sensor. Such a system would deny users access if their body temperature was not within range. In addition, [24] included motion sensing using a PIR sensor to prevent false detection, yet both papers cited code and hardware optimization as prime avenues for latency reduction and higher reliability.

Environmental factors such as lighting conditions continue to be a difficulty for the reliability of facial recognition systems. As [25] pointed out, measurements for performance in terms of speed and quality of recognition fall drastically under poor light conditions, justifying the need for adaptive algorithms and pre-processing images to enhance robustness in operational contexts.

Table 1 presents the comparative benefits of the various biometric technologies. It is obvious that while facial recognition promises higher scalability, usage convenience, and automation. It offers more flexibility, allowing easy authentication with limited drawbacks [26], a reasonable range of operation, and ease of integration to modern technology such as IoT, although the efficiency could be affected by facial occlusion and lightning conditions [27] and [28]. Also, apart from the high-cost computational power requirement, privacy and security concerns might arise due to the need to store data.

Table 1. Comparison of Biometric Methods

Biometric Method	Advantages	Disadvantages
Fingerprint Recognition	High accuracy, cost-effective	Requires physical contact, hygiene concerns
Iris Recognition	Extremely precise, difficult to spoof	Requires user cooperation, expensive hardware
Facial Recognition	Contactless, fast, AI-enhanced accuracy	Sensitive to lighting conditions, privacy concerns
Voice Recognition	Hands-free, remote authentication is possible	Accuracy is affected by background noise, voice changes

In conclusion, leveraging edge AI and cloud computing, facial recognition systems based on IoT can perform authentication locally to reduce latency and improve efficiency and security [29]. However, the vulnerability of the network and cyber-attacks pose a threat to IoT-based security solutions; with proper encryption and authentication processes, this can be mitigated [30].

3. METHOD

The actualization of the proposed system was through the development of a physical prototype model. The block diagram in Figure 1 was used as an architectural framework that represented the entire system. The block diagram consists of two main parts, revealing a physical hardware interface housing a Pi camera that captures users' faces. The faces are received by an edge device, which is an ESP32 module. The edge device provides the computational capabilities that run an embedded machine learning algorithm that performs facial classifications and compares with locally stored pre-trained facial images used for recognition of every face instance. The edge device also provides computational power that connects to a cloud interface.

The second part of the architecture is the integrated cloud interface, which provides remote storage of usage data and analytics. The analyzed data also provides additional intelligence and control of the door for the local door and provides remote monitoring. Control signals are released from the cloud interface to control an electromechanical actuator that activates the door opening and locking. Depending on the outcome of the facial recognition analysis, if the face is recognized, the door opens; otherwise, the door remains locked.

Table 2. Hardware Design Specification

S/N	Component	Voltage Rating(V)	Current Rating (A)	Power (Iv) (W)	Source
1	Esp32-CAM Wi-fi Module	3.3	0.18	0.594	All about electronics
2	Solenoid Load	12	0.6	8.4	All about electronics
3	LED	2	0.022	0.044	All about electronics
TOTAL			0.802	9.038	

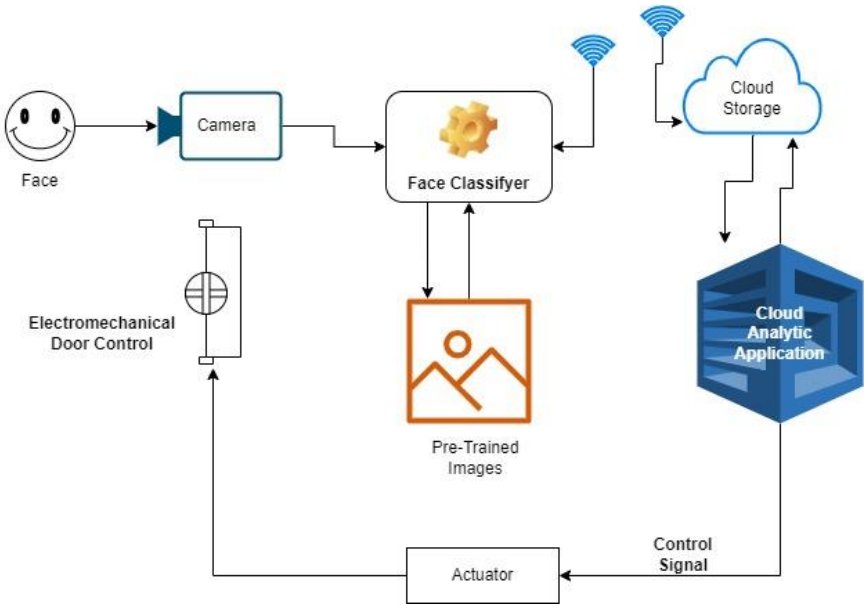


Figure 1. Architectural framework of the system

The edge device was actualized by implementing the circuit diagram in Figure 2, which was designed to the specifications listed in Table 2. The table shows that an ESP32-CAM board with embedded Wi-Fi feature was used. The board is rated at a 3.3 to 5 volt range, with a maximum current rating of 0.18 A, and a power rating of 0.594 W. The door was designed using a solenoid valve, rated at 14 volts, 0.6 A, and 8.4 W. This was connected to the main board using a 12 V electromechanical relay switch. Light Emitting Diode (LED) was used as an indicator that shows a successful face recognition, the door opens and otherwise. The LED is rated at 2 V, 0.022 A, and 0.004 W.

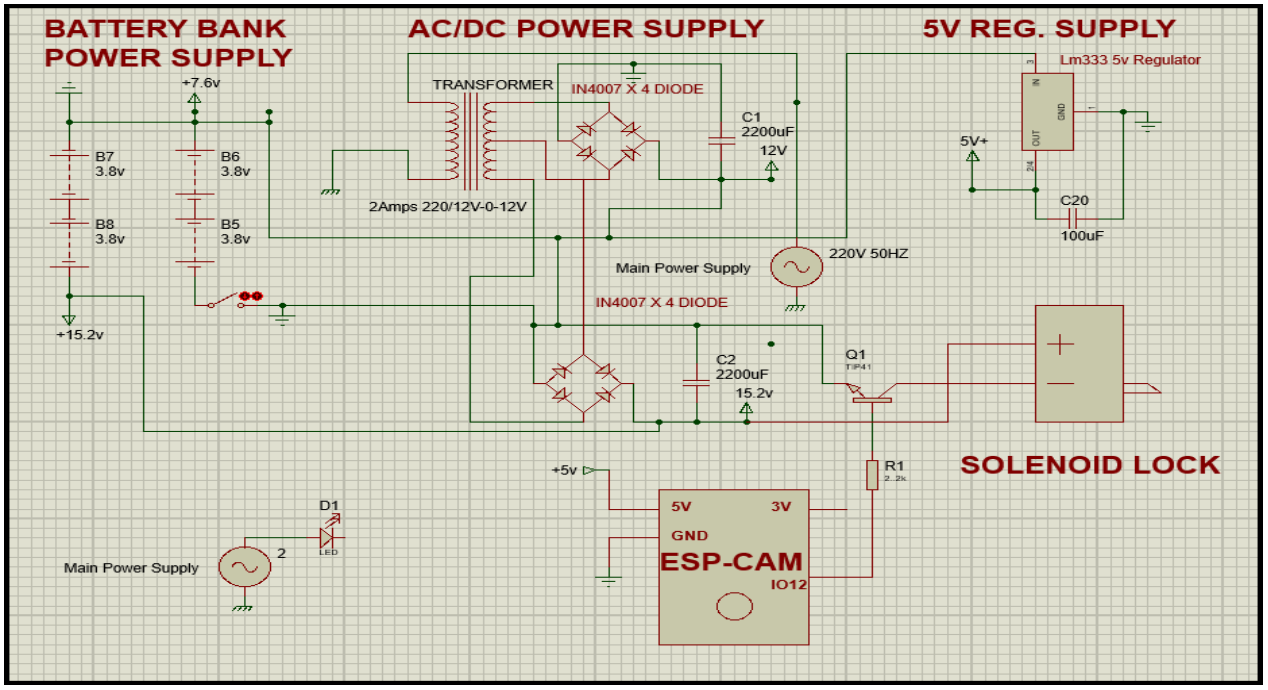


Figure 2. System's circuit Diagram

The face classifier algorithm used was the Haar cascade algorithm due to its ability to balance between speed and efficiency on constrained devices in real-time. The process used by this algorithm is illustrated in Figure 3.

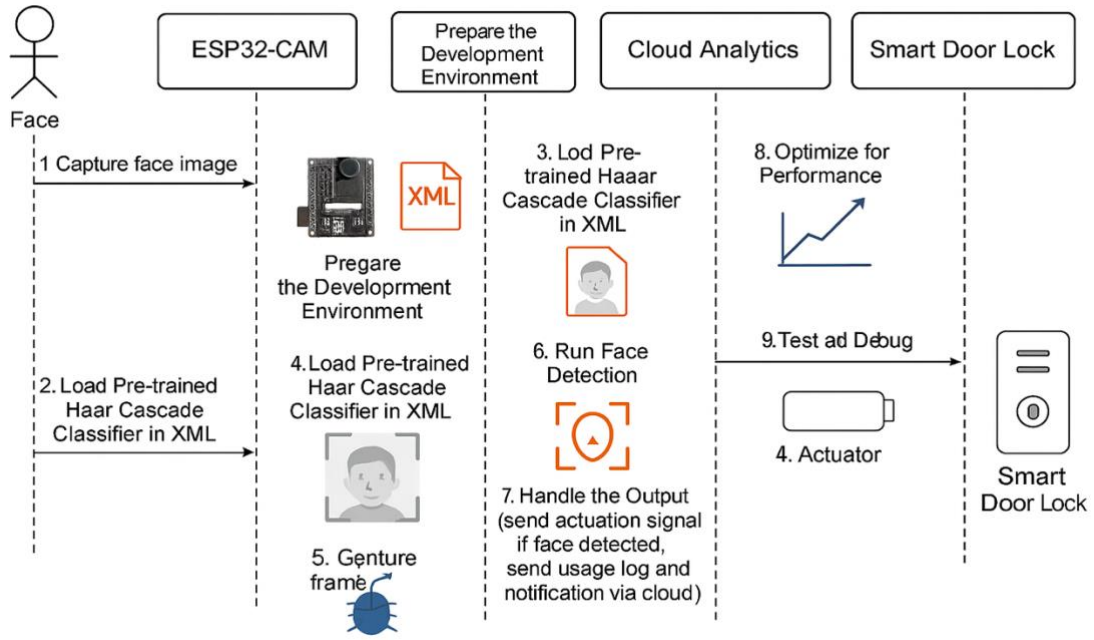


Figure 3. The process of implementing Haar Cascade

In Figure 3, captured photos are initially converted into grayscale to reduce computational complexity, then processed through a pre-trained XML classifier to scan for distinctive facial features. Upon successful identification, the system unlocks the smart lock and, concurrently, sends usage logs and notifications via a cloud interface that provides remote data monitoring and access control. Cloud analytics also play a crucial role in system parameter tuning, latency control, and enhancing recognition robustness under varying environmental conditions, such that the solution is maintained light while being adaptive for embedded IoT applications.

3.1. Systems Testing

To evaluate the performance of the smart door lock system with facial recognition as proposed herein, systematic testing in well-controlled environments was conducted. System implementation was through the ESP32-CAM module and a pre-trained Haar Cascade classifier capable of frontal face detection. The experiments focused on three primary performance criteria, which involved detection rate, processing latency, and CPU use. Environmental as well as operating condition response of the system was also evaluated to determine its feasibility.

Testing was divided into four categories:

- Tests were performed in well-lit and low-light conditions to measure the impact of light on performance when recognizing.
- The subjects were placed at various facial orientations, such as partial profiles and with obstructions such as face masks or glasses.
- ESP32-CAM was configured to take pictures at 320x240, 640x480, and 800x600 resolutions to ascertain the trade-off between processing time and recognition quality.
- Six experiments under each condition were conducted in which a registered subject attempted to enter the system. Detection results, processing time, and CPU usage were captured through the onboard debug interface and system logs.

4. RESULTS AND DISCUSSION

The results of the test conducted are presented based on the test metrics in the experiment. First, the response time under the different test conditions and six different test events is presented in Figure 4, the CPU load under these conditions is presented in Figure 5, and the accuracy plot is presented in Figure 6. The average test results are summarily presented in Table 3, showing the average detection time, CPU load, and accuracies across the six test scenarios.

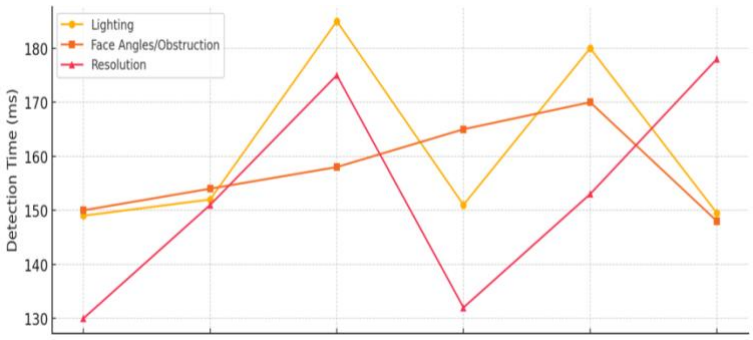


Figure 4. Time Duration Across Different Conditions

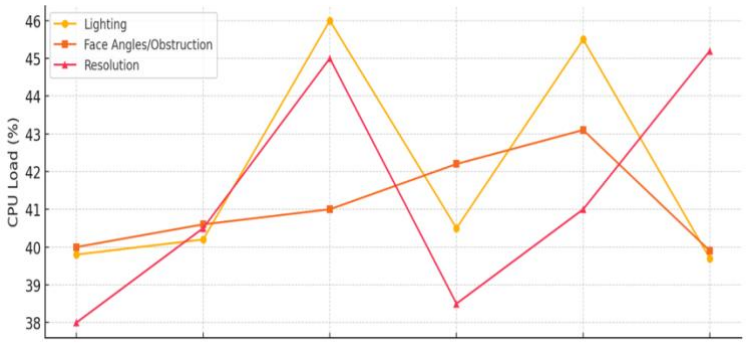


Figure 5. CPU Load Across Different Conditions

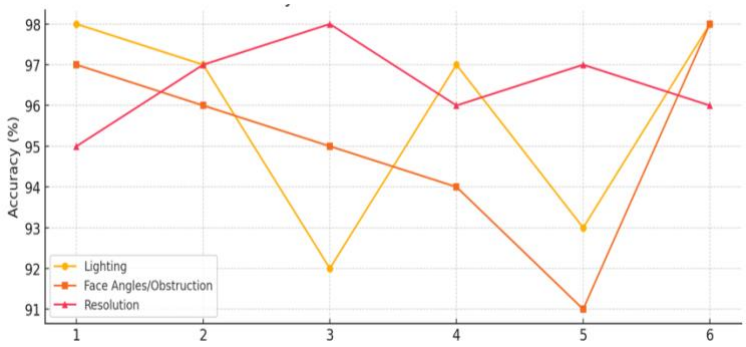


Figure 6. Accuracy Across Different Test Conditions

Table 3. Test Results

Condition	Avg. Detection Time (ms)	Avg. CPU Load (%)	Avg. accuracy (%)
Good Lighting	151.25	40.5	97.0
Poor Lighting	182.5	45.8	92.5
Face Obstruction	158.0	41.5	94.2
Low Resolution (320×240)	131.0	38.2	95.5
Medium Resolution (640×480)	151.0	40.8	97.0
High Resolution (800×600)	176.5	45.1	96.0

4.1. Discussion

The test results indicate that an average detection time of 151.25 milliseconds was recorded alongside an average accuracy of 97%, and a tolerable CPU load of 40.5%. This is a good threshold for real-time smart access control systems in many areas of application. Performance on adverse lighting degraded fairly well, with detection time increased to 182.5 ms and accuracy reduced to 92.5%, as expected of Haar

Cascade's proven vulnerability to low-contrast inputs. Such rates, however, remain within non-critical access acceptable requirements.

The system was found to be stable with moderate facial obstructions and changes in orientation and was 94.2% accurate on average, suggesting that the algorithm is stable against actual variations such as users wearing spectacles or leaning their heads slightly. Computationally, the system processed low-resolution frames with minor latency (131 ms) and CPU usage (38.2%), although with a slight reduction in accuracy. High-resolution frames increased recognition accuracy at the expense of higher latency (176.5 ms) and CPU usage (45.1%). This is the trade-off between recognition quality and computation, and suggests that the system can be dynamically controlled by power supply or required speed. Secondly, the cloud analytics interface served to enhance system functionality further by logging, remote monitoring, and parameter optimisation without overloading embedded hardware.

This result, when compared to those of existing literature, shows a great improvement on both efficiency and time of detection. For example, [19] achieved an accuracy of 90% with a face recognition time of 15 seconds, which is quite lower than the performance of our system. Again, although the work of [18] achieved 99% accuracy, the latency (0.6 seconds) of face recognition is still quite higher compared to ours. While neither did report on the CPU load as a benchmark, our work achieved a considerable CPU load balance with improved efficiency and very low latency. This will shape the view of embedded AI on constrained devices.

5. CONCLUSION

This work presents the design, development, and performance evaluation of a Haar Cascade algorithm and ESP32-CAM embedded board-based facial recognition smart door lock system. The system captures real-time users' facial images and controls the door opening and locking mechanism through cloud-based computation for improved actuation and monitoring for autonomous access. Testing under various conditions, such as lighting conditions, facial orientation, and resolution levels, the system achieved a high recognition rate of 97%, a mean detection time of 151.25 milliseconds, and an acceptable CPU utilisation of 40.5%, confirming its suitability for low-power IoT applications. The results affirm that the Haar Cascade algorithm, although computationally lighter than deep learning-based solutions, can be made to perform well if it is specially optimised for embedded systems. Incorporation of cloud capabilities makes the system more scalable through the provision of remote access, data logging, and immediate alerts. Nevertheless, the study also outlines areas of weakness that involve a lack of sensitivity to low light and facial occlusions. In conclusion, the work offers a cost-effective, contactless, and scalable method for modern home- and small-office-scale access control systems. Aspects that may be targeted by subsequent research include integrating more sophisticated machine learning architecture (e.g., CNN), adaptive lighting adjustment compensation, and encrypted biometric data processing towards ensuring improved robustness, privacy, and implementation feasibility.

DATA AVAILABILITY STATEMENT

The data presented in this study are available on request from the corresponding author.

CONFLICTS OF INTEREST

The authors of this work declare that they have no conflicts of interest.

REFERENCES

[1] K. N. Sai, D. T. Sunil, and D. M. Eshwarappa, “A comprehensive review of door lock security systems,” *Int J Circuit, Comput Netw*, vol. 5, no. 1, pp. 12–17, Jan. 2024, doi: 10.33545/27075923.2024.v5.i1a.61.

[2] V. D. Babu, R. R. Dornala, C. Anusha, P. R. Babu, K. K. Mohan, and K. V. Sumanth, “A Hybrid Multimodal Biometric Recognition System (HMBRS) based on Fusion of Iris, Face, and Finger Vein Traits,” in *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)*, IEEE, Sep. 2024, pp. 1287–1292. doi: 10.1109/ICOSEC61587.2024.10722340.

[3] G. V. Kumari, K. C. N. Raju, Y. S. Prasanna, K. M, M. P. Kumar, and K. Gorji, “Facial Recognition through Enhanced Access Control System with OTP Verification,” in *2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, IEEE, Nov. 2024, pp. 1409–1412. doi: 10.1109/ICDICI62993.2024.10810767.

[4] R. V. Virgil Petrescu, “Face Recognition as a Biometric Application,” *J Mechatronics Robot*, vol. 3, no. 1, pp. 237–257, Jan. 2019, doi: 10.3844/jmrsp.2019.237.257.

[5] M. Gomez-Barrero *et al.*, “Biometrics in the Era of COVID-19: Challenges and Opportunities,” *IEEE Trans Technol Soc*, vol. 3, no. 4, pp. 307–322, Dec. 2022, doi: 10.1109/TTS.2022.3203571.

[6] A. Fola-Rose, E. Solomon, K. Bryant, and A. Woubie, “A Systematic Review of Facial Recognition Methods: Advancements, Applications, and Ethical Dilemmas,” in *2024 IEEE International Conference on Information Reuse and Integration for Data Science (IRI)*, IEEE, Aug. 2024, pp. 314–319. doi:

10.1109/IRI62200.2024.00070.

[7] M. A. Febriantono, A. Zuhair, and Khaeruddin, "Smart Home Security System Using Face Recognition Based on IoT- CNN," in *2023 International Conference on Information Technology Research and Innovation (ICITRI)*, IEEE, Aug. 2023, pp. 28–33. doi: 10.1109/ICITRI59340.2023.10249929.

[8] J. Krishna Chaithanya, G. A. E. Satish Kumar, and T. Ramasri, "IoT-Based Embedded Smart Lock Control Using Face Recognition System," 2019, pp. 1089–1098. doi: 10.1007/978-3-030-00665-5_104.

[9] Prof. Dr. Paul Mccullagh, "Face detection by using Haar Cascade Classifier," *Wasit J Comput Math Sci*, vol. 2, no. 1, pp. 1–5, Mar. 2023, doi: 10.31185/wjcm.109.

[10] J. J. Teule, M. F. Hensel, V. Buttner, J. V. Sorensen, M. Melgaard, and R. L. Olsen, "Examining the Cyber Security of a Real World Access Control Implementation," in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, IEEE, Jun. 2020, pp. 1–3. doi: 10.1109/CyberSA49311.2020.9139617.

[11] A. Parsovs, "Estonian electronic identity card: Security flaws in key management," *Proc 29th USENIX Secur Symp*, 2020.

[12] Warda Hassan and Nosheen Sabahat, "Towards Secure Identification: A Comparative Analysis of Biometric Authentication Techniques," *VFAST Trans Softw Eng*, vol. 12, no. 1, pp. 105–120, Mar. 2024, doi: 10.21015/vtse.v12i1.1745.

[13] Mohd. Maroof Siddiqui, "AI-Based Human Face Recognition System," *J Electr Syst*, vol. 20, no. 11s, pp. 357–362, Nov. 2024, doi: 10.52783/jes.7174.

[14] A. S. Kumar, P. S. Sai, B. Parvathi, H. S. Manasa, and K. S, "Face Detection Approaches Using AI," in *2023 International Conference on Data Science and Network Security (ICDSNS)*, IEEE, Jul. 2023, pp. 1–6. doi: 10.1109/ICDSNS58469.2023.10245563.

[15] Rutuja Bankar, Nikita Bargat, Isha Hanmante, and Prof. Hemlata Dakore, "Face Recognition Using Facenet Deep Learning Network for Attendance System," *Int J Sci Res Comput Sci Eng Inf Technol*, pp. 458–463, Dec. 2022, doi: 10.32628/CSEIT228630.

[16] M. Yashashwini, K. S. Kumar, R. Pitchai, K. S. Sai Sankeerth, G. Arun Prasath, and D. Trinath, "Face Recognition Based Smart Door Lock System using Convolution Neural Network," in *2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)*, IEEE, Nov. 2023, pp. 1–6. doi: 10.1109/RMKMATE59243.2023.10368950.

[17] D. A. Wangean, S. Setyawan, F. I. Maulana, G. Pangestu, and C. Huda, "Development of Real-Time Face Recognition for Smart Door Lock Security System using Haar Cascade and OpenCV LBPH Face Recognizer," in *2023 International Conference on Computer Science, Information Technology and Engineering (ICCoSITE)*, IEEE, Feb. 2023, pp. 506–510. doi: 10.1109/ICCoSITE57641.2023.10127753.

[18] T.-N. Do, C.-L. Le, and M.-S. Nguyen, "IoT-Based Security With Facial Recognition Smart Lock System," in *2021 15th International Conference on Advanced Computing and Applications (ACOMP)*, IEEE, Nov. 2021, pp. 181–185. doi: 10.1109/ACOMP53746.2021.00032.

[19] P. E. U. Ekwueme, E. Okowa, "Facial Recognition Based Smart Door Lock System," *FUPRE J Sci Ind Res*, vol. 6, no. 2, 2022.

[20] P. K. Goyal, M. Giri, and S. Verma, "IoT-Based Smart Door Lock System with Face Recognition Using ESP32 CAM and Android App," 2024, pp. 365–376. doi: 10.1007/978-981-99-8661-3_27.

[21] S. A. Radzi, M. K. M. F. Alif, Y. N. Athirah, A. S. Jaafar, A. H. Norihan, and M. S. Saleha, "IoT based facial recognition door access control home security system using raspberry pi," *Int J Power Electron Drive Syst*, vol. 11, no. 1, p. 417, Mar. 2020, doi: 10.11591/ijpeds.v11.i1.pp417-424.

[22] J. S. Sonamoni *et al.*, "IoT-Based Smart Remote Door Lock and Monitoring System Using an Android Application," in *1st International Conference on Industrial, Manufacturing, and Process Engineering (ICIMP-2024)*, Basel Switzerland: MDPI, Nov. 2024, p. 85. doi: 10.3390/engproc2024076085.

[23] S. Sharma, M. Sharma, G. Sharma, and A. Bhasney, "IoT-Enabled Smart Door Lock System Using Temperature Sensor," in *2024 2nd International Conference on Disruptive Technologies (ICDT)*, IEEE, Mar. 2024, pp. 360–365. doi: 10.1109/ICDT61202.2024.10489006.

[24] G. R. Venkatakrishnan, "Sdafar: Iot Based Smart Door Automation Using Face Recognition in Computer Vision," *African J Biomed Res*, pp. 4856–4861, Dec. 2024, doi: 10.53555/AJBR.v27i4S.4492.

[25] F. L. Murjitama *et al.*, "The Smart Door Lock Using Face Recognition Access Based on Internet Of Things (IoT)," *Teknika*, vol. 13, no. 2, pp. 199–203, Jun. 2024, doi: 10.34148/teknika.v13i2.816.

[26] S. O. Olayemi, O. S. Olatunde, I. W. Oladimeji, and I. Folasade, "ENHANCING AUTHENTICATION EFFICIENCY IN COMPUTER-BASED EXAMINATIONS THROUGH ADVANCED FACE RECOGNITION SYSTEMS," *J Digit Secur Forensics*, vol. 1, no. 1, Aug. 2024, doi: 10.29121/digisecforensics.v1.i1.2024.24.

[27] F. Firdous, S. Bashir, S. Z. Rufai, and S. Kumar, "Integration of Artificial Intelligence and Internet of Things Technology in Classroom Attendance Systems.," in *2023 Seventh International Conference on Image Information Processing (ICIIP)*, IEEE, Nov. 2023, pp. 271–276. doi: 10.1109/ICIIP61524.2023.10537709.

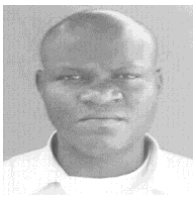
[28] A. P. S. Shekhawat, A. Chaurasiya, P. Chaurasiya, P. K. Patel, P. Pal, and S. K. Singh, "Realization of Smart and Highly Efficient IoTbased Surveillance System using Facial Recognition on FPGA," in *2022 International Conference on Futuristic Technologies (INCOFT)*, IEEE, Nov. 2022, pp. 1–5. doi: 10.1109/INCOFT55651.2022.10094500.

[29] X. Zhou and S. L. Keoh, "Deployment of Facial Recognition Models at the Edge: A Feasibility Study," in *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, IEEE, Sep. 2020, pp. 214–219.

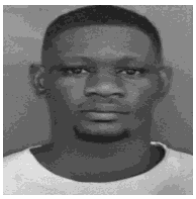
doi: 10.23919/APNOMS50412.2020.9236972.

[30] L. Cambosuela, M. Kaur, and R. Astya, "The Vulnerabilities and Risks of Implementing Internet of Things (IoT) in Cyber Security," in *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, IEEE, Mar. 2024, pp. 1–5. doi: 10.1109/ICRITO61523.2024.10522460.

BIOGRAPHIES OF AUTHORS



Chukwuemeka Obasi holds a PhD in digital electronics and computer engineering from the University of Nigeria in Nsukka, Nigeria in 2023, a masters of engineering (M. Eng) degree in Computer and Control engineering from the Nnamdi Azikiwe University in Awka, Nigeria in 2016, and a bachelor's of engineering degree (B. Eng) in Computer engineering from the Enugu State University of Science and Technology, Enugu, Nigeria. He is currently a senior lecturer at the Department of Computer Engineering, Edo University Iyamho, Edo State, Nigeria. His current research interests include robotics, cloud computing, biosensors, embedded systems, machine learning, human-centric computing, Intelligent systems, and the Internet of Things (IoT). He can be contacted at: chukwuemeka.obasi@edouniversity.edu.ng



Kasim Mohammed Tahir graduated from the Department of Computer Engineering, Edo State University, Iyamho, in the year 2024. He is currently serving in the compulsory National Youth Service Corp (NYSC) in Nigeria. He hopes to pursue a Master's degree as soon as he completes the service year. He can be contacted at: kasimtahir60@gmail.com