International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-14 Issue-10, September 2025

A Revolutionary Approach to Smart Applications Using IoT: Two-Level Authentication for Automatic Safety Door and Main Door Unlocking System using IoT and Deep Learning

Rinkuben N. Patel, Dharmen B. Shah, Mayurdhwajsinh B. Gohil

Abstract: ***The increasing adoption of innovative door systems in residential and commercial usage has improved convenience in accessing the doors, but also introduced new security threats. Conventional approaches, such as facial recognition or pin code-based authentication, often rely on single-layer mechanisms, which can be vulnerable to intrusions. This paper proposes a two-level authentication framework to enhance door security and reliability. The primary level utilises facial recognition to grant access through a security door to registered users, including family members, authorised personnel, and trusted visitors. The second level secures the main entry door, which unlocks exclusively for recognized family members, thereby introducing an additional layer of protection. A key contribution of this approach is its ability to perform facial recognition once and leverage the verified data across both security stages, reducing redundancy while strengthening overall access control. The proposed system demonstrates the potential to improve innovative security solutions by integrating multi-layered authentication for enhanced safety in residential and office environments.***

Keywords: Internet of Things, IoT, Smart Devices, Automation, Advancement, IoT Security and Risk

Abbreviations:
AI: Artificial Intelligence
CNN: Convolutional Neural Network
DL: Deep Learning
FLD: Fisher Linear Discriminant
HTTPS: Hyper Text Transfer Protocol Secure
IoT: Internet of Things
MQTT: Message Queuing Telemetry Transport
KNN: K-Nearest Neighbor
LBPH: Local Binary Patterns Histogram
OCR: Optical Character Recognition
PCA: Principal Component Analysis
SVM: Support Vector Machine
TLS/SSL: Transport Layer Security / Secure Sockets Layer
CCTV: Closed-Circuit Television
PIN: Personal Identification Number

Manuscript received on 20 August 2025 | First Revised Manuscript received on 29 August 2025 | Second Revised Manuscript received on 02 September 2025 | Manuscript Accepted on 15 September 2025 | Manuscript published on 30 September 2025.

*Correspondence Author(s)
Ms. Rinkuben N. Patel*, Department of Computer Science, Veer Narmad South Gujarat University, Surat (G.J), India. Email: rinks.npatel@gmail.com, ORCID ID: 0000-0001-9178-3554
Mr. Dharmen B. Shah, Department of Computer Science, Veer Narmad South Gujarat University, Surat (G.J), India. Email: dharmenbshah@gmail.com
Mr. Mayurdhwajsinh B. Gohil, Department of Computer Science, Veer Narmad South Gujarat University, Surat (G.J), India. Email: mayursinh2001@yahoo.co.in

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open-access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

I. INTRODUCTION

Crime rates are increasing day by day, and with the rising crime rate, home and office security is a must nowadays, as known individuals commit many crimes. IoT-based smart home systems have already been launched in the market [1]. Various research is ongoing on innovative applications of IoT. Researchers have defined challenges such as power management [2], data security, real-time data handling [3], data management and integration [4], deploying nanoscale devices for sensing and communication [5], remote access [6], and integrating sensor-sensed data with software [7]. Today, various home surveillance systems are available on the market, but home surveillance remains challenging, particularly when tracking a subject through CCTV images. Therefore, it is necessary to install a security system capable of preventing unwanted entry. Many digital technologies have already been invented and deployed in a market where doors open based on scanned fingerprints. A digital locking and unlocking system where one can set the security pin and lock and unlock it by using the security code. Smart Chip cards are also used for unlocking doors, but they come with the risk of card loss, where someone can easily access your system if the card is stolen or lost. Iris scanners, thumb scanners, and face recognisers are blooming in the market for safety-driven installations [8]. However, none of these methods is good enough to secure our homes and offices. A stolen password or smart card can easily gain access to the system [9]. The fingerprint scanner is also vulnerable. Additionally, hiring a security guard can be very expensive for homes and small businesses. A cost-effective surveillance system needs to be developed [10]

The proposed surveillance and alert system aim to address the need for cost-effective security solutions by utilizing microcomputers and machine learning technology. This system is designed to be compatible with existing camera systems and capable of delivering satisfactory performance.

The key components of the proposed system include tiny. IoT devices equipped with deep learning capabilities.

These devices will analyze inputted and captured images from the cameras using advanced comparison and recognition algorithms. By leveraging machine learning techniques, the system can learn and adapt over time, improving its ability to detect and alert users about potential security threats. This approach provides a more efficient and proactive method for monitoring premises, enhancing overall security without the need for expensive infrastructure or personnel. Overall, the proposed surveillance and alert system represents a cost-effective and scalable solution to address the challenges of modern-day security threats, leveraging advanced technology to provide adequate surveillance and timely alerts.

II. RELATED REVIEW

The vision of IoT is comprehensive. IoT is integrated with image processing, natural language processing, data analytics and computer vision as the future of technology [11]. One crucial aspect of computer vision is image processing, which involves the manipulation and analysis of digital images. In image processing, computers apply various algorithms and methods to perform tasks such as enhancing image quality, detecting objects or patterns within images, and extracting useful information from images for further analysis. Image processing techniques can range from basic operations, such as resizing and cropping images, to more advanced tasks, including edge detection, image segmentation, object recognition, and content-based image retrieval.

Facial recognition is a method within image processing that focuses on capturing and identifying human faces. One of the techniques used in facial recognition is the Eigenface algorithm. This algorithm creates what are called Eigenfaces, which are essentially mathematical representations of faces. These Eigenfaces form a space where facial recognition is performed by projecting input faces onto this space and analyzing them in a simplified, dimensionally reduced manner.

The Eigenface algorithm enables a comprehensive analysis of faces, capturing key features and patterns that facilitate the recognition and identification of individuals. It's a powerful tool in the field of facial recognition and has been utilised in various applications, including security systems and biometric authentication.

Lo-Wei et al state that eigenGS bridges PCA and 2D Gaussian image representations through a transformation pipeline that enables instant, frequency-aware initialization of Gaussian parameters. It achieves faster convergence, higher reconstruction quality, and better generalization with fewer parameters, making it suitable for real-time image applications [12].

The Fisher linear discriminant (FLD) seeks to find projections on a line. This class-specific method classifies classes by identifying features that can be used for classification, and aims to create inter-class and intra-class scattering [13].

Haar-Cascade Classifiers, such as Viola-Jones, identify and detect features of a human face, including ears, two eyes, a Nose, and a Mouth. It was proposed by Alfred Haar in 1909, which is similar to convolutional kernels. Different Haar features include 2 Rectangular Haar features, 3 Rectangular Haar features, and 4 Rectangular Haar features, also known as Edge features and Line Features. Using these features, we can perform matrix calculations to identify a particular image region [14].

The Support Vector Machine (SVM) is a supervised learning model associated with a specific learning algorithm. SVM analyses data for classification and regression. SVM separates categories by a clear margin. Using the Kernel trick, it performs non-linear classification. It is capable of delivering high classification accuracy. The algorithm is used for image classification, text classification, digit classification, and object classification [15].

Convolutional neural networks (CNNs) have achieved remarkable success across various fields, including medical research, and an increasing interest has emerged in radiology. It is composed of convolution layers, pooling layers, and fully connected layers and is designed in a way that automatically and adaptively learns spatial hierarchies of features through a backpropagation algorithm [16].

K-Nearest Neighbour (KNN) is a supervised machine learning algorithm primarily used for classification purposes. KNN classifies the dataset using a training model, similar to a testing query, by considering the k nearest training data points that are neighbours. And at last, the algorithm performs a vote to determine which classification needs to be finalised [17].

Fahim Faisal and Syed Akhter Hossain have developed a smart door lock using face recognition that uses the Viola-Jones method, and face recognition is implemented using the PCA, where the door unlocks for a known person and triggers an alarm for an unknown person. They have achieved 95% accuracy in recognition in fluorescent lighting conditions [18].

Ijaradar et al. have developed a cost-effective real-time Security Surveillance System that utilises Raspberry Pi and computer vision. Haar Cascade and LBPH algorithm are used for recognition of a face and achieved more than 70% of accuracy in normal light conditions [19].

By combining OpenCV, Raspberry Pi, and NodeMCU, you can create a versatile and cost-effective surveillance system capable of performing facial recognition and triggering alerts based on detected faces. This system can be customized and expanded further to meet specific requirements and integrate additional features as needed.

III. PROPOSED MODEL AND ALGORITHM

For the proposed work, an algorithm and flowchart are developed that are depicted in this section. Here's a step-by-step algorithm on how you can capture images of allowed users and train a dataset to recognize those images using OpenCV and Python:

A. Algorithm

Step 1: Capture images of allowed users using a camera and store them in a local dataset.

Step 2: Fetch all dataset images and

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

train the dataset to recognize the image

Step 3: Recognize the images and set a flag variable as KNOWN, UNKNOWN, AND FAMILY MEMBERS.

Step 4: If the flag is set to UNKNOWN, send the images to the Application for recognition. If the Admin accepts the photos, store the pictures in the Dataset and update the flag to 'KNOWN' or 'FAMILY MEMBER'; otherwise, proceed to step No. 7.

Step 5: If the flag is set to KNOWN, send the Flag to the IoT device to unlock the Outer Safety Door.

Step 6: If the flag is set to FAMILY MEMBERS, send the Flag to the IoT device to unlock the Outer Safety Door. And send a flag to the Inner Main door to perform the unlock.

Step 7: If the UNKNOW flag is detected, then call for security action.

Step 8: End

B. Mathematical Model

DSimages[n]- Images in a Dataset
CPimages[n]– Captured Images
RECImage[n]- Recognized Image set
UNKNWImages[n]- Unknown Image set
KNWImages[n]- Known Image set
FAMILYImages[n]- Family Members Image Set
FLAG0 – For Known images set
FLAG1 – For Family Members images set
FLAG0-1– For the Unknown images set,
Images Captured and Need to be Processed CPimages[n]– Captured Images

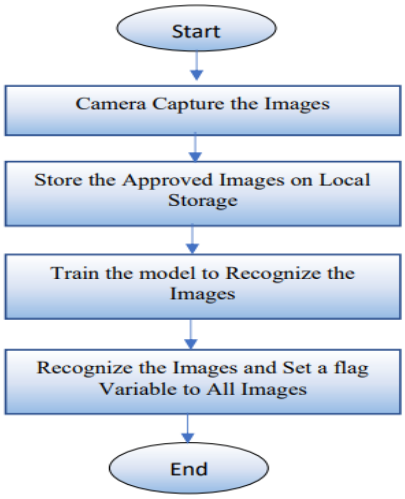
Were,

CPimages[n]v = {All captured images by camera}
UNKNWImages[n] = {FLAG0-1}
KNWImages[n] = {FLAG0 + FLAG1}
FAMILYImages[n] = {FLAG1}

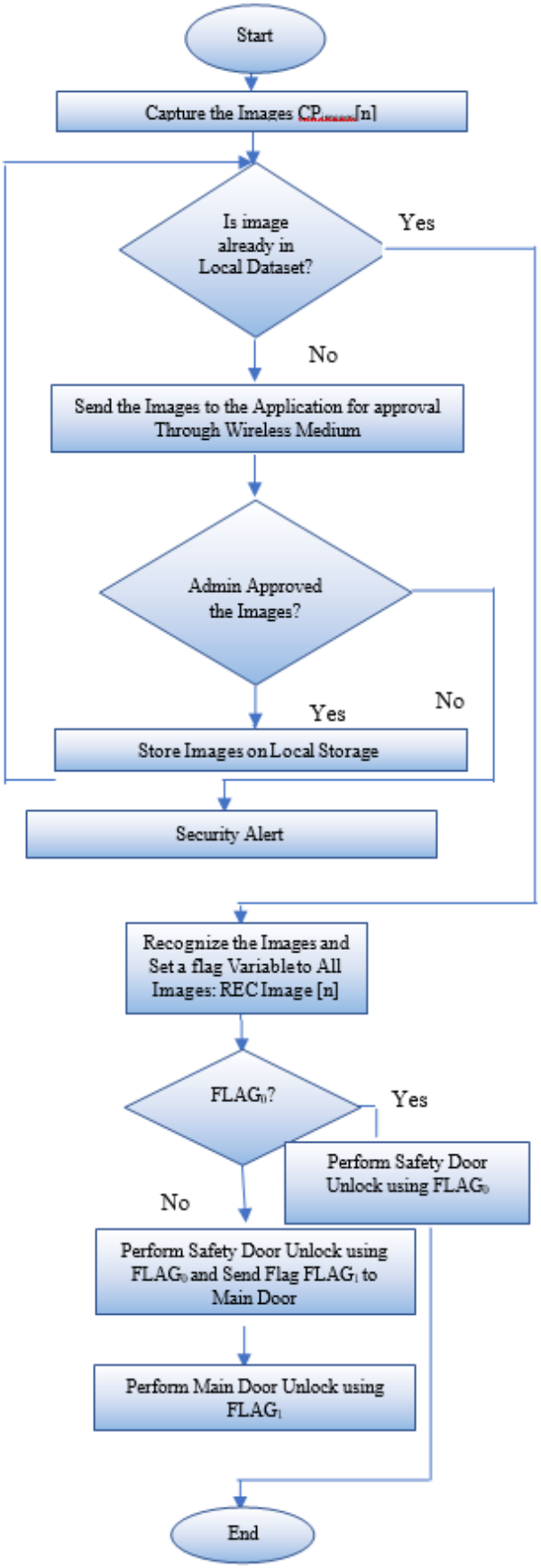
Image Stored in a database = RECImage[n]- Recognized Image set
Where,RECImage[n]={KNWImages[n]+ FAMILYImages[n] }
Images For Security Alert = UNKNWImages[n]

C. Model Flow Chart

Flowchart 1 is for application usage, and Flowchart 2 is for model training, which utilises the dataset to train the model.



Flowchart 1: Flowchart of Application Usage



Flowchart 2: Flowchart of Model Training

© Copyright: All rights reserved.

IV. IMPLEMENTATION

The prototype design and development is divided into four segments namely dataset creation, train the dataset, image recognition and image upload, and hardware action.

A. Dataset Creation

Creating a dataset is a crucial aspect of research, as it forms the foundation for any study. Images can be imported from the available library or captured by the camera at a different angle with varying illumination and stored in a dataset. Images may require admin permission for new users. It is necessary to perform image processing before finalising the dataset, as for face recognition, the image of a face should be cropped. For that image processing, the face detection algorithm will work. Multiple photos of the same person, taken from different angles, are required for further processing. Once the dataset is ready, it is further assigned to the training model.

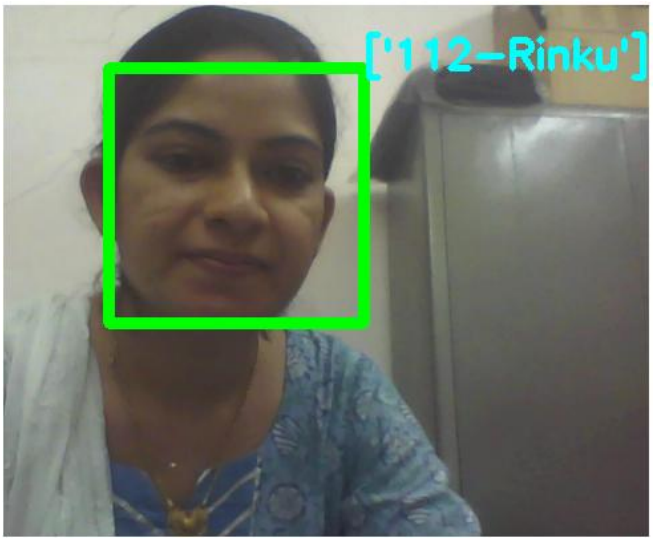
[Fig.1: Camera-Captured Image for the Dataset]

B. Train the dataset

For training, the algorithm needs to extract the face features. A unique face ID is generated and trained by the machine, assigning labels based on the face ID. A unique identification number is given to each individual in a dataset. In the training model, it loads the image, converts it to grayscale, and then converts that image into a NumPy array to obtain the ID from the image. After that, the system extracts the face from the training image sample and retrieves the ID from the image.

C. Image Recognition and Image Upload

Images from the local dataset are used for the reorganisation of an object, whereas a new image set is uploaded to the cloud for administrative permission. Various functions are already available based on the selected reorganization model. In OpenCV, the LBPH Face Recognizer_create() function is used for object recognition, which generates a Local Binary Pattern Histogram. Once the face is recognized an action is performed based on the recognized image. The flag variable is set for each recognised image and sends a signal to the IoT program to initiate further action. If a face is present, append it to the list along with its ID. If the recognition model identifies an image, then set a person's name in a variable and send a signal to the IoT program with a positive signal to perform the door open action based on the value set in the person's name variable to decide whether to open only the safety door or both the safety and main doors.



[Fig.2: Image Recognition]

D. Hardware Action

If the Flag is set to 'KNOWN person', then the outer safety door will be open, and the flag variable will be sent to an internal system for main door action. If a flag is set for a family member, it is also set for both the outer safety door and the internal main door to perform the unlock action. And if a flag is set to the UNKNOWN flag, a security alarm will be triggered.

V. SECURITY AND RISK CONCERN

The integration of machine learning and IoT indeed holds great potential, but security concerns are paramount, especially when the system is connected to the internet [20] Here's how you can address the mentioned security concerns and ensure the reliability of the proposed model:

Data Encryption: To mitigate the risk of data interception and unauthorized access, ensure that all data transmitted over the internet is encrypted using strong encryption protocols. Use secure communication channels such as HTTPS or MQTT with TLS/SSL for data transfer between devices and the cloud. Implement end-to-end encryption to protect sensitive data, such as facial images and authentication tokens, from being compromised.

Internet Connectivity Reliability: Recognize that internet connectivity is crucial for the system's functionality, especially for real-time access control based on facial recognition. Implement robust error-handling mechanisms to handle intermittent internet connectivity issues gracefully. Consider implementing offline fallback mechanisms or local caching of authentication data to ensure uninterrupted operation even in the event of internet connectivity loss.

Facial Recognition Algorithm: Utilize a robust facial recognition algorithm that can effectively handle ambient variations, such as changes in lighting conditions, face

© Copyright: All rights reserved.

orientation, and image blurring. Deep learning-based algorithms, such as convolutional neural networks (CNNs), are well-suited for this task as they can automatically learn and adapt to different environmental conditions. Additionally, consider preprocessing techniques such as image normalization and feature extraction to enhance the robustness of the facial recognition system.

Privacy Protection: Implement privacy-preserving measures to safeguard user data and ensure compliance with data protection regulations. Minimise the storage and retention of sensitive data to the extent necessary for the system's functionality. Provide users with control over their data, including the ability to opt out of data collection and request the deletion of stored data. Regularly audit the system for potential privacy vulnerabilities and address any identified issues promptly.

By addressing these security concerns and implementing appropriate safeguards, you can enhance the security and reliability of the proposed IoT-based facial recognition system while ensuring user privacy and data protection.

VI. RESULT AND DISCUSSION

The provided text outlines the process and observations related to dataset creation, facial recognition accuracy, and door unlocking timings in an experimental setup. Here's a summary of the key points:

Table I: Face Recognition Experiment with Different Parameters

No. of images in Dataset /Sec	Camera Capacity	Distance	Angle	Time
70	1.0MP	~½ Feet	~160-180	~0.8-1.05 Sec
70	1.0MP	~½ Feet	~80-120	~0.8-1.50 Sec
70	1.0MP	~1 Feet	~160-180	~1.10-1.40 Sec
70	1.0MP	~1 Feet	~80-120	~1.10-1.60 Sec
70	1.0MP	~1.5 Feet	~160-180	~1.10-1.40 Sec
70	1.0MP	~1.5 Feet	~80-120	~1.50-1.90 Sec
70	1.0MP	~1.75 Feet	~160-180	~1.10-1.60 Sec
70	1.0MP	~1.75 Feet	~80-120	~1.50-2.00 Sec
70	1.0MP	~2 Feet	~160-180	~1.30-1.60 Sec
70	1.0MP	~2 Feet	~80-120	~1.40-2.50 Sec

The provided text outlines the process and observations related to dataset creation, facial recognition accuracy, and door unlocking timings in an experimental setup. Here's a summary of the key points:

A. Dataset Creation

Seventy images are captured from the camera in one second for the dataset generation. Only 20 images are displayed in Figure 1 (assumed to be a part of the dataset).

Camera Specifications: The camera used for testing the model is a 1.0MP camera.

Facial Recognition Accuracy: Trained images are recognized with higher accuracy. Recognition accuracy is influenced by factors such as the Distance between the camera and the person's face. Accuracy is higher when the person is closer to the camera (approximately 1ft to 1.5ft). Recognition may take longer for individuals standing farther away (beyond 1.5 feet). Angle of the person's face when capturing images for training the dataset and recognising them. Brightness and camera quality also impact accuracy.

B. Door Unlocking Timings

Once the person is recognized, it takes 1 to 3 seconds to open the door. The system identifies the type of image and performs the appropriate action (e.g., unlocking the outer safety door or the main door). For error handling, if the person's image is not recognised, the system sends an email to the registered email address. Further actions are performed based on the operation selected in the application.

The accuracy of recognition and door unlocking timings depends on several factors, including the angle of the person's face, the distance from the camera, lighting conditions, and the camera's quality. To achieve higher accuracy, attention should be paid to these factors during dataset creation and system testing.

VII. CONCLUSION

The proposed work aims to enhance security for family members and small offices by providing two layers of physical security. This approach can help reduce the risk of theft and unwanted entries. Both microcontrollers and microcomputers can be utilized based on their specific requirements. While numerous security applications are already available on the market, the focus here is on developing cost-effective solutions that are both affordable and provide adequate security measures. These applications should offer different levels of security based on the categorization of captured images. By categorising captured images, the system can distinguish between authorised individuals (such as family members or trusted personnel) and unauthorised individuals. This categorization can be based on various factors, such as facial recognition, biometric data, or predefined access permissions. The implementation of two physical layers of security adds an extra level of protection, enhancing the overall security posture of homes and small offices. Additionally, by focusing on cost-effectiveness, these solutions can be accessible to a broader range of users, ensuring that security measures are not only effective but also affordable and practical. Overall, the text offers insights into the experimental setup, observations, and factors that influence the accuracy and performance of the facial recognition and door unlocking system. These findings can be valuable for optimizing the system and improving its real-world effectiveness.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to everyone who contributed to the successful completion of this research. Special thanks are due to our colleagues and friends for their constant motivation and assistance throughout the research process. We are grateful to DCS and VNSGU for providing the necessary resources and facilities. Finally, we would like to thank our families for their unwavering support and patience throughout this journey.

© Copyright: All rights reserved.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/Competing Interests:** Based on my understanding, this article does not have any conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organisation or agency. The independence of this research is a crucial factor in affirming its impartiality, as it was conducted without any external influence.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The data and materials supporting the findings of this article are publicly accessible.
- **Author's Contributions: Ms. Rinkuben N. Patel** contributed to the conceptualisation and methodology, with a focus on the development of IoT. **Mr. Dharmen B. Shah** was responsible for data collection, data analysis, and image processing. **Mr. Mayurdhwajsinh B. Gohil** contributed to image processing, mobile application development, and drafting and revising the manuscript. All authors reviewed and approved the final version of the manuscript and take responsibility for its content.

REFERENCES

1. B. Zia and K. Chauhan, "A Research Paper on Internet of Things based upon Smart Homes with Security Risk Assessment using OCTAVE Allegro," International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 06, Jun. 2020. DOI: http://dx.doi.org/10.17577/IJERTV9IS060692
2. G. Y. Odongo, R. Musabe, D. Hanyurwimfura, and A. D. Bakari, "An Efficient LoRa-Enabled Smart Fault Detection and Monitoring Platform for the Power Distribution System Using Self-Powered IoT Devices," IEEE Access, vol. 10, Jul. 2022. DOI: https://doi.org/10.1109/ACCESS.2022.3189002.
3. O. Said, Y. Albagory, M. Nofal, and F. Al Raddady, "IoT-RTP and IoT-RTCP: Adaptive Protocols for Multimedia Transmission over the Internet of Things Environments," IEEE Access, vol. 5, Sep. 2017. DOI: https://doi.org/10.1109/ACCESS.2017.2726902
4. S. N. Swamy and S. R. Kota, "An Empirical Study on System Level Aspects of the Internet of Things (IoT)," IEEE Access, vol. 8, Oct. 2020. DOI: https://doi.org/10.1109/ACCESS.2020.3029847
5. M. A. C. Alvarado and P. Bazán, "Understanding the Internet of Nano Things: overview, trends, and challenges," e-Ciencias de la Información, vol. 9, no. 1, Jun. 2019. DOI: https://doi.org/10.15517/eci.v1i1.33807
6. M. Ishaq, M. H. Afzal, S. Tahir, and K. Ullah, "A Compact Study of Recent Trends of Challenges and Opportunities in Integrating the Internet of Things (IoT) and Cloud Computing," International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), IEEE, 2021. DOI: 1https://doi.org/10.1109/ICECube53880.2021.9628191
7. S. Siddiqui, S. Hameed, S. A. Shah, I. Ahmad, A. Aneiba, D. Draheim, and S. Dustdar, "Toward Software-Defined Networking-Based IoT Frameworks: A Systematic Literature Review, Taxonomy, Open Challenges and Prospects," IEEE Access, vol. 8, Jul. 2020. DOI: https://doi.org/10.1109/ACCESS.2022.3188311
8. M. G. Samaila, J. B. F. Sequeiros, T. Simões, M. M. Freire, and P. R. M. Inácio, "IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space," IEEE Access, vol. 10, Jan. 2020. DOI: https://doi.org/10.1109/ACCESS.2020.2965925
9. A.-R. H. Hussein, "Internet of Things (IoT): Research Challenges and Future Applications," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 10, no. 6, 2019. LINK DOI: http://dx.doi.org/10.14569/IJACSA.2019.0100611
10. S. A. Nama and K. A. Neamah, "Securing the Internet of Things," Texas Journal of Engineering and Technology, vol. 7, no. 3, 2022.LINK: https://zienjournals.com/index.php/tjet/article/view/943
11. S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," Journal of Big Data, vol. 6, 2019. DOI: https://doi.org/10.1186/s40537-019-0268-2
12. L. -W. Tai, C.-E. Li, C.-L. Chen, C.-J. Tsai, H.-T. Chen and T. -L. Liu, "EigenGS Representation: From Eigenspace to Gaussian Image Space," *2025 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Nashville, TN, USA, 2025, pp. 13487-13496, DOI: https://doi.org/10.1109/CVPR52734.2025.01259
13. R. Rahim, T. Afriliansyah, H. Winata, D. Nofriansyah, Ratnadewi, and S. Aryza, "Research of Face Recognition with Fisher Linear Discriminant," 4th International Conference on Operational Research (InteriOR), IOP Conf. Series: Materials Science and Engineering, vol. 300, 2018, p. 012037. DOI: 10.1088/1757-899X/300/1/012037
14. Rahmad, C., & Andrie, R. (2020). Comparison of the Viola-Jones Haar Cascade Classifier and Histogram of Oriented Gradients (HOG) for Face Detection. *IOP Conference Series: Materials Science and Engineering, 732*(1), 012038. DOI: https://doi.org/10.1088/1757-899X/732/1/012038
15. J. Cervantes, F. García-Lamont, L. Rodríguez-Mazahua, and A. López-Chau, "A comprehensive survey on support vector machine classification: Applications, challenges and trends," *Neurocomputing*, vol. 408, pp. 189–215, May 2020. DOI: https://doi.org/10.1016/j.neucom.2019.10.118
16. R. Yamashita, M. Nishio, R. K. G. Do, and K. Togashi, "Convolutional neural networks: an overview and application in radiology," Insights into Imaging, vol. 9, pp. 611–629, 2018. DOI: https://doi.org/10.1007/s13244-018-0639-9
17. S. Uddin, I. Haque, H. Lu, M. A. Moni, and E. Gide, "Comparative performance analysis of K nearest neighbour (KNN) algorithm and its different variants for disease prediction," Scientific Reports, vol. 12, p. 6256, 2022. DOI: https://doi.org/10.1038/s41598-022-10358-x
18. F. Faisal and S. A. Hossain, "Smart security system using face recognition on Raspberry Pi," 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), 2019, pp. 1–8. DOI: https://doi.org/10.1109/SKIMA47702.2019.8982466
19. J. Ijaradar and J. Xu, "A Cost-efficient Real-time Security Surveillance System Based on Facial Recognition Using Raspberry Pi and OpenCV," Current Journal of Applied Science and Technology, vol. 41, no. 53, Apr. 2022. DOI: https://doi.org/10.9734/cjast/2022/v41i531665
20. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges," IEEE Access, vol. 9, Apr. 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3070555

AUTHOR'S PROFILE

Ms. Rinkuben N. Patel is an Assistant Professor in the Department of Computer Science at VNSGU, Surat, Gujarat, India. She has participated in various National Conferences, seminars and training programs. She has published six research papers in a leading journal. She has completed her Bachelor of Computer Applications degree. She has completed her Post-Graduation in Master of Computer Applications. Her Doctoral research is in Wireless Sensor networks. She is an enthusiastic academic with a strong academic track record. She has over 12 years of experience in the educational field.

Mr. Dharmen B. Shah is a Skilled academician with 18+ years of teaching experience. He successfully cleared the UGC NET examination in 2012, demonstrating his strong foundation in his field. Currently, he is pursuing doctoral research focused on Optical Character Recognition at Veer Narmad South Gujarat University. His research contributes to advancements in this specialized area. Mr. Shah's academic interests span multiple domains, including Image Processing, Internet of Things (IoT), Mobile Development, and Web Development. His diverse expertise allows him to engage in interdisciplinary projects and stay updated with the latest technological trends. Through his teaching and research, Mr. Shah continues to make significant contributions to both the academic community and the development of innovative technologies.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Mr. Mayurdhwajsinh B. Gohil is an Assistant Professor in the Department of Computer Science at Veer Narmad South Gujarat University, Surat, where he has been serving since April 2017. With over 18 years of teaching experience, he has made significant contributions to postgraduate education. He successfully cleared the GSET examination. His academic career spans more than a decade, during which he has developed expertise in various computer science subjects. Mr. Gohil is dedicated to fostering student learning and engagement through innovative teaching methods. He actively participates in curriculum development and research activities within the department. Mr. Gohil's academic and research interests encompass Digital Image Processing, Natural Language Processing, Internet of Things (IoT), Cloud Computing, and Mobile Application Development. His commitment to academic excellence and continuous professional growth makes him a valuable member of the university faculty.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

© Copyright: All rights reserved.