

Integrated Deep Learning System for Secure and Intelligent Smart Home Access Control

Mr. Siva Ramakrishna Sani¹, Mohammad Sameer², Peketi Naveen³ and Bezawada Naga Venkata Reddy⁴

¹Assistant Professor, Department of Artificial Intelligence and Data Science, Lakireddy Bali reddy College of Engineering, Mylavaram -521230, Andhra Pradesh, India

Email: ssrk102@gmail.com

²⁻⁴B. Tech Student, Department of Artificial Intelligence and Data Science, Lakireddy Bali reddy College of Engineering, Mylavaram -521230, Andhra Pradesh, India

Email: sameermd12q@gmail.com, peketinaveen87@gmail.com, reddybezawada7@gmail.com

Abstract—The rapid advancement of smart home technology necessitates sophisticated and integrated solutions for enhanced security and seamless user experience. The Integrated Deep Learning System for Enhanced Door Access Security introduces an innovative approach to home access control by integrating real-time communication technologies with deep learning methodologies. This system leverages advanced image and video analytics powered by deep learning algorithms to improve visitor authentication accuracy. Key features include adaptive learning models for dynamic threat detection and predictive visitor behavior analysis, ensuring robust security while maintaining user convenience. A web-based interface enables secure voice, text, and video communication between homeowners and visitors, facilitating real-time interaction and remote access management. This paper presents the system's architecture, distinctive features, and implementation strategies, highlighting its ability to provide proactive security measures, intelligent guest management, and continuous real-time monitoring. By merging security and communication into a unified, user-centric platform, this solution addresses the growing demand for advanced remote access control and interactive engagement in modern smart homes.

Keywords—Smart Home Security, Deep Learning, Door Access Control, Real-time Monitoring, Adaptive Learning Models, Video Analytics, Voice and Text Communication, Remote Access Control.

I. INTRODUCTION

In today's rapidly evolving world, security has become a critical aspect of safeguarding homes, offices, and other private spaces. As traditional security mechanisms such as locks and alarms increasingly become insufficient, there is an urgent need for more sophisticated, intelligent solutions that provide both convenience and enhanced protection.

Access control systems, particularly those designed to monitor and regulate entry into physical spaces, form the cornerstone of modern security infrastructure. However, these systems, although effective, often lack the real-time interaction, intelligence, and adaptability needed to cope with the challenges posed by advanced intruders or unexpected situations.

The new “Integrated Deep Learning System for Improved Door Access Security” [?] project applies deep learning to fill that hole with a modern solution, which uses deep-learning algorithms and sophisticated two-way communication from real-time video surveillance systems to strengthen door access security. Integrated with cutting-edge computer vision and audio processing technologies, the system offers a perfect way of interaction between the homeowner and visitor at door. Instead of depending on just visual recognition or conventional [1] entry mechanisms, this project aimed to build an ultimate security system providing smart decision-making, real-time alerts and voice communication but with further layering the robustness impressions safety as well ease.

The core component of this project is image recognition based on deep learning [2], which can help the system recognize who is coming to the door and who it might be. It will screen between authorized entities, such as family members, friends, or trusted visitors, and unknown persons using advanced face recognition algorithms. In addition, the system has motion detection, able to identify abnormal activity near the door.

automatically creating alerts and video capture. It would guarantee real-time, adaptive responses in case a security breach may occur, for example, an unknown individual trying to penetrate the premises. Besides traditional video surveillance, the system also allows for audio processing capabilities and can have two-way communication [3] with a person at the door as well as a homeowner. In addition, through a web-based interface, homeowners are able to have voice conversations with visitors to screen deliveries, screen unknown callers, or confirm appointments without ever having to get up and open the door. This interaction is also one step in helping the homeowner gain more control over decisions regarding access, so that they can easily determine whether or not to allow someone access or report any suspicious activity. This project will aim at providing an integrated security solution that involves more than surveillance systems [4]: intelligent analysis, interactive communication, and real-time monitoring. It is aimed at smooth operations in multiple conditions and ensuring that performance is the same regardless of day or night conditions. This solution also takes into consideration the limitation in staying at home all the time and thus makes sure that such people will have a chance to monitor the requests for door access wherever they are. This system unifies artificial intelligence with real-time communication [5] to provide more dependable, adaptive, and efficient solutions for home and office security. It is hoped to increase the user’s experience with intuitive and accessible systems that increase safety and reduce risk, giving users much peace of mind with respect to their homes.

The overall goal is to strengthen security at door-access points [6] and expand the scope of what a modern security system could be capable of. It’s designed using deep learning, audio/video communication, and cloud technologies in a manner that makes the system sophisticated yet user-friendly for the protection of people, their families, and businesses from unauthorized access and threats. With the increased utilization of smart technologies in homes and business operations, this research project lays the groundwork for future advances in the development of smart integrated security systems that are more responsive and accessible than ever. This paper is structured to present a comprehensive survey of existing literature related to the topic. In Section 3, the proposed work and methodology for the project are detailed, providing a clear outline of the approach used. The methodology itself is thoroughly described in Section 4, ensuring that the process is well-understood. Section 5 concludes the paper, summarizing the key findings, while Section 6 compiles the references and cited works that contributed to the research

II. LITERATURE SURVEY

Integration of various technologies in home security has been a highly researched and developed area. Different systems have been proposed addressing various aspects of security from video surveillance to access control and real-time communication. The literature below is some of the most relevant contributions in the field of smart security systems, giving an insight into the use of machine learning, facial recognition, IoT [7], and voice interaction in improving door access security. Image-Based Surveillance System [8] This paper proposes an image-based surveillance system for improving home security. This system gives notice to the homeowner when someone gets to the door. It mainly uses machine learning techniques, facial recognition, in identifying the visitor through video capture. Homeowners see the identity of the visitor and can communicate directly with the visitor – a feature of added safety and convenience. This means the system would be developed to ensure it is accessible on a smartphone, allowing for flexibility and instant accessibility of surveillance data. It also integrates automatic facial recognition using video capture and processing, making it one of the most responsive solutions for modern homes.

Integration of Voice Image Recognition for Smart Home Security [9] This paper examines integrating voice and image recognition to augment smart home security. The system, therefore, utilizes OpenCV for image processing and PyAudio for voice recognition, hence authenticating visitors through face and voice. Microsoft Azure

supports back-end processing of all the recognition tasks incorporated into it. This two-layer recognition ensures that only individuals who can be identified by their features and voice pattern will have the access. It is shown how a single system can be more secure by using more than one type of biometric authentication simultaneously rather than relying solely on one specific method Facial Recognition Home Security System [10] The project aims to automate home security by integrating facial recognition with the Internet of Things (IoT) features. Video data captured during this is processed for facial identification. The main processing unit is a Raspberry Pi. It is intended to make the safety of homes more advanced by being able to automatically recognize visitors and inform the owners of possible security breach. Combining the features from both facial recognition and IoT, this solution to home security goes smooth and scalable.

Use of Smart Home Security Solutions via Facial Authentication and Speaker Recognition [11] The approach combines the use of facial and speaker recognition authentication. This way, it takes a much more holistic view toward home security. With its use of a Siamese neural network for facial recognition and a Gaussian Mixture Model for speaker recognition, the system provides an accuracy rate of 82.71%. This smart home security [12] solution is different as it accommodates masked and non-masked people to make it more flexible and applicable to reality. The system boasts total security as the two different biometric authentication methods used here minimize the chances of accessing by unauthorized personnel. Smart Security Surveillance Using IoT [13] It developed an IoT-based security system that captures pictures of visitors and automatically sends real-time alerts to the owner of the house. It is known to detect movement and automatically record pictures; hence, this enhances the monitoring capabilities of the conventional surveillance systems that are provided. This work highlights the application of IoT in home security by demonstrating how sensing and connected appliances can lead to a more sensitive and intelligent security solution.

A. IoT-Based Smart Home Security using Face Recognition

[15] This system integrates face recognition with an IoT infrastructure in order to automate the access control, alerting the user of a potential intruder. The entire process of face recognition maintains the security aspects as only authorized people gain access to the premises. The real-time communication and monitoring happen through the IoT framework. Face Recognition-Based Intelligent Smart Doorbell System with Advanced Security Improvements [14] This smart doorbell system allows for real-time face recognition at an accuracy of 94.53% using Raspberry Pi and OpenCV. Technology solution: this is an affordable home security system that does instant identification of visitors without manual interaction. Smart Surveillance with Smart Doorbell [16] [18]. The smart doorbell project uses the technology of IoT in taking photos of visitors and sending out alerts through email and SMS. In this way, home owners can see who is at their door in real time. Face Recognition and Voice Command Smart Door Unlock System. The current paper presents a smart door unlock system based on the idea of face recognition and voice commands for keyless entry; thus the system only allows entry to authorized users. Access without the use of physical keys, this is an intuitive yet secure access control [17]. Smart Home Security System with Face Recognition and Voice Command Designing [19] This system will integrate face recognition technology and voice commands to offer safe and keyless access to homes. Real-time notifications are sent over Telegram to ensure that homeowners are instantly alerted to attempted access. This creates a compounded authentication scheme providing both convenience and security, ensuring that people can pass through securely and have information on access events. Development of an IoT-based Facial Recognition Door Access Control Home Security System using Raspberry Pi. [21] This project integrates facial recognition with IoT and forms an intelligent access system that is responsive, providing the contribution to the high level of security within the access control system.

TABLE I: DETAILS OF TECHNOLOGIES AND IDENTIFIED GAPS

Title	Technology	Identified Gap
Image-based Surveillance System	Single Shot-Multipox Detector	Pre-defined messages, cloud dependency, heavy Raspberry Pi usage, OpenCV reliance
Combining Voice and Image Recognition for Smart Home Security System	OpenCV, PyAudio	Smart home security using Raspberry Pi, combining face and voice recognition for enhanced security and convenience

III. DATASET DESCRIPTION

- Preparing the Data for Face Recognition: The Celebrity Face Image Dataset, created by Kaggle and comprising 100 photos of each of the 18 Hollywood actors, was used by the face recognition module. We

included photos of a few team members to give the dataset greater relevance, making the model appropriate for both celebrities and non-celebrities.

- Preparing the Feature Extraction Process: We used the Multi-Task Cascaded Convolutional Neural Network [10] (MTCNN) for face detection and alignment, and we used particular facial feature points to align with the centers of each image. In order to improve performance, these photos were then normalized and resized to FaceNet-compatible sizes. In the end, 128-d matrices of feature vectors were generated from each image using the FaceNet architecture. These matrices would identify certain facial characteristics that might be utilized to distinguish between individuals.
- Preparing the Voice Recognition Data: The Speaker Recognition Audio Dataset, which we used for the speaker recognition module, was acquired from Kaggle and includes voice recordings for 50 speakers, each of which provided more than an hour of audio in WAV format. These MFCCs are essentially statistical features that describe the recorded sounds

IV. PROPOSED WORK

The proposed work will introduce an integrated deep learning system that ensures improved security access at doors by transforming ordinary home security mechanisms into a more smarter, secure, and user-friendly solution. In this multi-stack system with deep learning, it integrates facial recognition, voice authentication, IoT integration [22], and real-time communication to give the whole approach toward home access control. The system is designed to be not only highly secure but also user-friendly, so that the homeowners can authenticate visitors safely

The main objectives of the proposed system are:

- Facial Recognition for Visitor Identification:
- Voice Authentication for Secure Access:
- Real-Time Communication:
- It combines real-time monitoring and control with an IoT-based architecture.:
- Multi-Layered Authentication for Maximum Protection:
- User-Friendly Interface and Experience:
- Real-time Alerting and Notifications:
- Security and privacy:
- Scalability and Adaptability

A. Methodology

The Integrated Deep Learning System for Enhanced Door Access Security methodology is a step-by-step approach with in-depth implementation of the proposed system so that all aspects are designed and implemented very carefully. It explains the procedures of developing and integrating various aspects of the system, starting from data acquisition to system deployment.

System Architecture: This proposed system can be divided into two primary modules:

Deep Learning Model for Facial Recognition Voice Authentication System IoT-Based Communication [20] and Control User Interface for Real-Time Interactivity All these constituents would combine in such a way that the access management system to doors would be secure and efficient through a multi-modal authentication process

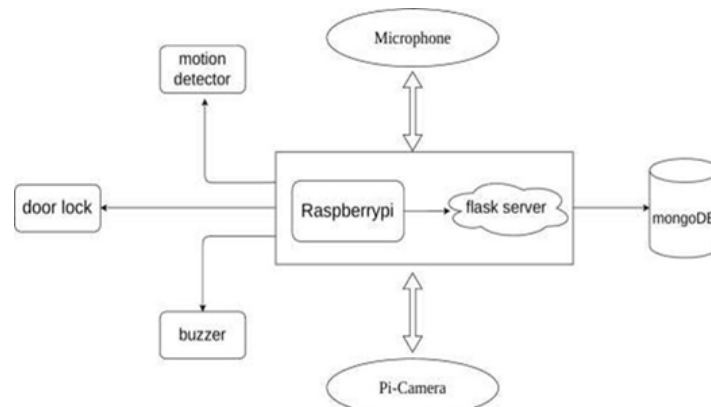


Figure 1: System model Architecture

Data Collection and Preprocessing

- **Facial Data Collection** This is going to be a facial recognition model trained on authorized images. There shall be several images of every individual in the database, captured under various lighting conditions, angles, and expressions. Techniques applied to these images include flipping, rotating, and scaling for data augmentation [23] so that the model generalizes well to every possible situation. Then, all these images are stored in an encrypted database.
- **Voice Data Acquisition** The same approach will be followed for voice identification. A set of voice recordings of registered individuals will be obtained through the use of a high quality microphone. The sample will include different speaking styles, emotional and not emotional content, and different levels of background noise to be very robust. The recorded voice samples will be converted into voiceprints which will then be kept safely and used as comparison during verification.
- **Face Identification Model** The facial recognition model was developed using Convolutional Neural Networks (CNNs), which are highly efficient for image data. The application utilized pre-trained models such as VGGFace2, FaceNet, and ResNet [24], fine-tuned on the gathered dataset. The model was trained to extract features from images containing faces and compare them with stored face templates to determine whether the visitor is authorized. This robust system ensures accurate recognition even under challenging conditions, such as variations in lighting and angles. Facial recognition process will be divided into the following steps
- **Face Detection:** Faces will be detected from the input video stream using MTCNN (Multi-task Cascaded Convolutional Networks), an advanced technique that ensures high accuracy in detecting faces from various angles and lighting conditions.
- **Feature Extraction:** After detection, facial features will be extracted using the FaceNet model, which is known for its powerful embedding technique that captures the unique characteristics of a face.
- **Face Matching:** The extracted features will then be compared with the stored database of authorized users.
- **Decision Making:** If a match is found, the system will make a decision to grant or deny access based on the recognition outcome

Voice Authentication Model

Using a Deep Neural Network and Hidden Markov Models would be necessary to perform voice recognition efficiently, thus requiring accurate voiceprints. PyAudio tools would capture the audio inputs, and the MFCC features would be used in voice analysis. The procedure related to voice authentication is as follows.

- **Voice Capture:** The system captures and processes the audio signal using PyAudio, ensuring high-quality audio data for further analysis.
- **Voiceprint Analysis:** Relevant features of the audio sample are extracted, forming a unique voiceprint using MFCC features. This step is crucial for distinguishing the characteristics of the speaker's voice.
- **Voice Match:** The extracted voiceprint is compared to those in the database of authorized users using the Gaussian Mixture Model (GMM). GMM helps in modeling the probability distributions of the voiceprint features, making the comparison more robust and accurate.
- **Access Control:** If the voiceprint matches one from an authorized user in the database, the system grants access.
- **Real-Time Communication and Video Streaming** A video streaming system will be used to achieve real-time interaction between the homeowner and the visitor. Video and audio streaming will be done low latency using WebRTC or RTSP protocol. This allows for real-time communication where the homeowner will visually identify the visitor, then interact through video and audio. The following components will be integrated for this feature:
- **Camera Interface:** Capture quality video feed from the camera in front of the door.
- **Video Streaming:** Send the video feed to the mobile app or web interface of the homeowner.
- **Audio Communication:** Provide two-way audio communication through a microphone and speaker setup.

IoT Integration

The system will utilize the IoT devices such as Raspberry Pi or Arduino to collect and send data to get real-time performance and control from a distant location. The IoT components shall include

- **Visitor Presence:** On detection of the presence of a visitor, activate cameras and sensors
- **Alert System:** Inform the homeowner regarding the visitors' presence with alerts and notifications through SMS or email or push notifications in an app
- **Door Lock Mechanism:** Transmit with the electronic locks on the door for access based on authentications. This shall enable the homeowner to lock or unlock doors from anywhere.

B. Integrate the System

All subsystems will be well integrated: face recognition, voice authentication, real-time communication, and IoT control.

Flask or Django will be applied for backend development to cater for the interaction between the different components.

The server will be well connected with the interfaces of both mobile and web applications in a fully integrated manner through RESTful APIs. The central controller [25] will run the IoT devices, which will then interface with the backend using the MQTT or HTTP protocols.

C. User Interface Development

Easy user-friendly usability and also accessibility will be ensured with the UI.

- Mobile Application: Built using Flutter or React Native wherein homeowners can get notified, view visitor images, and have real time communications with visitors. The Web Interface will provide a web dashboard for homeowners to alter the settings, monitor visitors, and get alerts Both interfaces-mobile and web-must availed of the following features:
- Live video feed: Voice message to a visitor in real time. Unlock the door remotely Administer user profiles and access controls

V. ALGORITHM

A “Integrated Deep Learning System for Enhanced Door Access Security” integrates image, audio, and deep learning technologies to secure access to doors through detection, recognition, and authentication of visitors. This system utilizes MTCNN as a face detector, FaceNet for face recognition, and GMM for voice recognition, thus ensuring multiple verification modes. Below are the algorithms that form the core of this project.

Algorithm 1: Visitor Detection and Face Capture [H] Visitor Detection and Face Capture

Input: None (triggered by motion sensor or doorbell) Output: DetectedFaces - List of cropped face images
CaptureAndDetect Activate Camera frame is being captured Detect faces using MTCNN and obtain bounding box coordinates Crop the image based on bounding boxes for each detected face DetectedFaces

Algorithm 2: Face Recognition with FaceNet [H] Face Recognition with FaceNet

Input: DetectedFaces - List of cropped face images Output: IdentifiedFaces - List of recognized identities (names or “Unknown”) RecognizeFaces Load Pre-trained FaceNet Model each face in DetectedFaces Generate a 128-dimensional embedding using FaceNet each embedding vector Compare with stored embeddings of authorized individuals similarity exceeds threshold Classify as authorized individual Label as “Unknown” IdentifiedFaces

Algorithm 3: Voice Recognition with GMM [H] Voice Recognition with GMM

Input: AudioClip - Audio recording of visitor’s voice Output: VoiceIdentity - Recognized voice identity (name or “Unknown”) RecognizeVoice Load GMM Voice Model Compute MFCC (Mel-Frequency Cepstral Coefficients) from AudioClip Input extracted features into the GMM model voice matches an authorized individual Label accordingly Classify as “Unknown” VoiceIdentity

Algorithm 4: Multi-Modal Identity Verification and Alert [H] Multi-Modal Identity Verification and Alert

Input: IdentifiedFaces, VoiceIdentity Output: Alert notification and communication log VerifyIdentity both IdentifiedFaces and VoiceIdentity match Confirm visitor’s identity one of the recognitions is “Unknown” Label visitor as “Partially Authorized” Classify as “Unknown Visitor” Generate Alert based on visitor classification visitor is partially or unrecognized Enable communication interface for the homeowner Log Communication for future analysis Alert Notification

Algorithm 5: System Performance Evaluation [H] System Performance Evaluation

Input: TestFaceData, TestVoiceData, GroundTruthFaces, GroundTruthVoices Output: Precision, Recall, and F1 Score metrics EvaluatePerformance Evaluate Face Recognition: Compare TestFaceData with GroundTruthFaces Evaluate Voice Recognition: Compare TestVoiceData with GroundTruthVoices Use confusion matrices to compute Precision, Recall, and F1 Score Evaluation Metrics

Algorithm 6: Full System Workflow for Enhanced Door Access Security [H] Full System Workflow for Enhanced Door Access Security

Input: None (automatic trigger by motion or doorbell) Output: System status, alerts, and communication log ExecuteWorkflow Execute Visitor Detection and Face Capture Execute Face Recognition on detected faces visitor speaks Capture audio and execute Voice Recognition Execute Multi-Modal Identity Verification and Alert Log Interaction Data in Security Database System Status and Alert Details

VI. EXPERIMENTAL RESULTS

The performance of the "Integrated Deep Learning System for Enhanced Door Access Security" was assessed across its primary components. The accuracy of each module was calculated using test datasets that simulated real-world conditions. The results indicate that the facial recognition module achieved the highest accuracy, while the voice authentication module also delivered reliable results

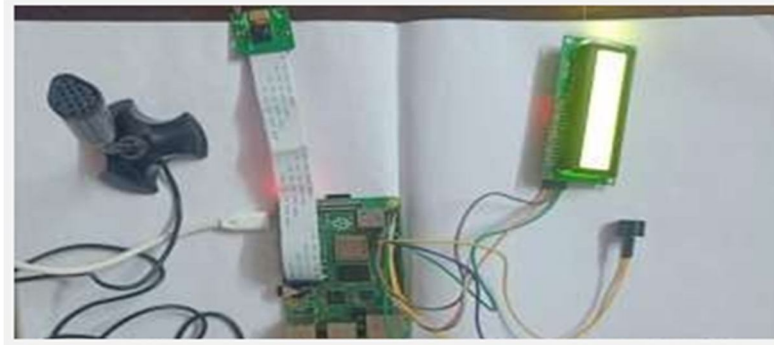


Figure 2: Working model Devices

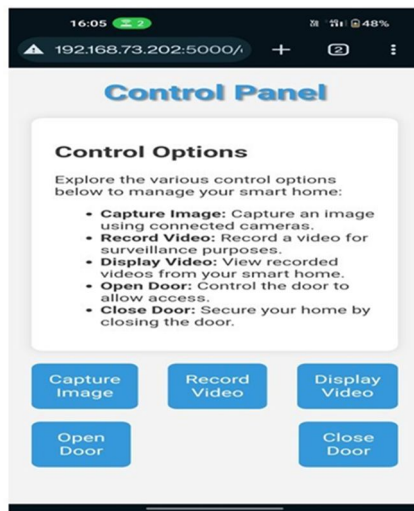


Figure 3: Home Page-Control panel

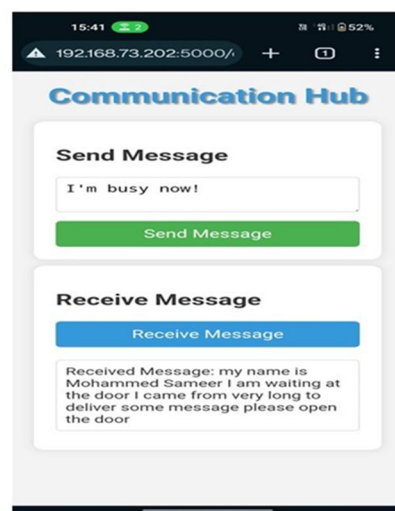


Figure 4: Communication Hub



Figure 5: Image Captured

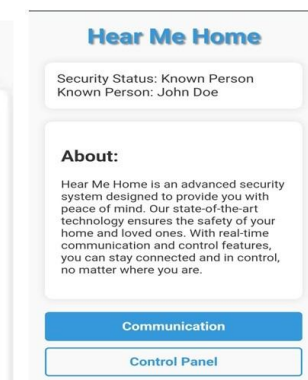


Figure 6.5: Result

VII. CONCLUSION

The "Advanced Deep Learning Framework for Secure and Intelligent Door Access in Smart Homes" marks a major leap in smart home security. Utilizing a multi-modal system with MTCNN for precise face detection,

FaceNet for reliable face recognition, and Gaussian Mixture Models (GMM) for accurate voice verification, it offers a comprehensive security solution beyond traditional methods. By integrating facial and voice recognition, it ensures highly accurate, real-time verification while maintaining user convenience. Additionally, its seamless communication interface allows homeowners to interact with visitors, adding human oversight to the automated system. This study highlights the effectiveness of AI-powered multi-modal authentication in residential security and paves the way for future advancements incorporating additional biometric and contextual data. The project establishes a foundation for developing intelligent, adaptive, and robust security frameworks for both residential and commercial use.

REFERENCES

- [1] A. M. Zeki, E. E. Eldaw, A. A. Ibrahim, C. Haruna, and S. Abdulkareem, "Automatic Interactive Security Monitoring System," 2013 International Conference on Research and Innovation in Information Systems (ICRIIS), 2013, pp. 215-220, doi: 10.1109/ICRIIS.2013.6716711.
- [2] G. Kang, H. Seong, D. Lee, and D. H. Shim, "A Versatile Door Opening System with Mobile Manipulator through Adaptive Position-Force Control and Reinforcement Learning," *Robotics and Autonomous Systems*, vol. 180, 2024, doi: 10.1016/j.robot.2024.104760.
- [3] P. Gayathri, A. Stalin, and S. Anand, "Intelligent Smart Home Security System: A Deep Learning Approach," 2022 IEEE 10th Region 10 Humanitarian Technology Conference (R10-HTC), 2022, pp. 438-444, doi: 10.1109/R10-HTC54060.2022.9929516.
- [4] H. Wu, H. Han, X. Wang, and S. Sun, "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey," *IEEE Access*, vol. 8, 2020, pp. 153826-153848, doi: 10.1109/ACCESS.2020.3018170.
- [5] M. Schmitt, "Securing the Digital World: Protecting Smart Infrastructures and Digital Industries with Artificial Intelligence (AI)-Enabled Malware and Intrusion Detection," *Journal of Industrial Information Integration*, vol. 36, 2023, p. 100520, doi: 10.1016/j.jii.2023.100520.
- [6] C.-L. Zhong, Z. Zhu, and R.-G. Huang, "Study on the IoT Architecture and Gateway Technology," 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), 2015, pp. 196-199, doi: 10.1109/DCABES.2015.56.
- [7] B. M. M. El-Basioni and S. M. A. El-Kader, "Laying the Foundations for an IoT Reference Architecture for Agricultural Application Domain," *IEEE Access*, vol. 8, 2020, pp. 190194-190230, doi: 10.1109/ACCESS.2020.3031634.
- [8] K. Albulayhi, A. A. Smadi, F. T. Sheldon, and R. K. Abercrombie, "IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses," *Sensors*, vol. 21, no. 19, p. 6432, 2021, doi: 10.3390/s21196432.
- [9] J. Guth, U. Breitenbücher, M. Falkenthal, F. Leymann, and L. Reinfurt, "Comparison of IoT Platform Architectures: A Field Study Based on a Reference Architecture," 2016 Cloudification of the Internet of Things (CIoT), 2016, pp. 1-6, doi: 10.1109/CIOT.2016.7872918.
- [10] J. Deogirikar and A. Vidhate, "Security Attacks in IoT: A Survey," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 32-37, doi: 10.1109/I-SMAC.2017.8058363.
- [11] M. O'Neill, "Insecurity by Design: Today's IoT Device Security Problem," *Engineering*, vol. 2, pp. 48-49, Mar. 2016, doi: 10.1016/J.ENG.2016.01.014.
- [12] G. Sharma, S. Vidalis, N. Anand, C. Menon, and S. Kumar, "A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open Issues," *Electronics*, vol. 10, no. 19, p. 2365, 2021, doi: 10.3390/electronics10192365.
- [13] ETSI CYBER, "Cyber Security for Consumer Internet of Things," ETSI Sophia Antipolis, France, 2019.
- [14] ETSI CYBER, "Cyber Security for Consumer Internet of Things: Baseline Requirements," ETSI TS, vol. 103, no. 645, pp. V1, 2019.
- [15] N. K. Suryadevara, S. C. Mukhopadhyay, S. D. T. Kelly, and S. P. S. Gill, "WSN-Based Smart Sensors and Actuator for Power Management in Intelligent Buildings," *IEEE/ASME Transactions on Mechatronics*, vol. 20, no. 2, pp. 564-571, 2014.
- [16] M. P. uris'ic', Z. Tafa, G. Dimic', and V. Milutinovic', "A Survey of Military Applications of Wireless Sensor Networks," 2012 Mediterranean Conference on Embedded Computing (MECO), 2012, pp. 196-199.
- [17] Y. Sankarasubramaniam, I. F. Akyildiz, W. Su, and E. Cayirci, "Wireless Sensor Networks: A Survey," *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002.
- [18] A. Demaille, S. Peyronnet, and B. Sigoure, "Modeling of Sensor Networks Using XRM," Second International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA 2006), 2006, pp. 271-276.
- [19] S. Fatima, N. Aiman Aslam, I. Tariq, and N. Ali, "Home Security and Automation Based on Internet of Things: A Comprehensive Review," *IOP Conference Series: Materials Science and Engineering*, vol. 899, no. 1, p. 012011, Jul. 2020, doi: 10.1088/1757-899X/899/1/012011.
- [20] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," 2015 Internet Technologies and Applications (ITA), 2015, pp. 219-224.
- [21] H. M. Aldosari, "A Proposed Security Layer for the Internet of Things Communication Reference Model," *Procedia Computer Science*, vol. 65, pp. 95-98, 2015.

- [22] A. H. Abed, M. Nasr, and B. Sayed, "The Principle Internet of Things (IoT) Security Techniques Framework Based on Seven Levels IoT's Reference Model," in *Internet of Things—Applications and Future: Proceedings of ITAF 2019*, Springer, 2020, pp. 219-237.
- [23] J. De Loof et al., "Internet of Things-Architecture IoT-A Deliverable D1.5-Final Architectural Reference Model for the IoT V3.0," *IoT-A (257521)*, pp. 1-499, 2013.
- [24] M. A. G. Santos et al., "Online Heart Monitoring Systems on the Internet of Health Things Environments: A Survey, a Reference Model and an Outlook," *Information Fusion*, vol. 53, pp. 222-239, 2020.
- [25] M. R. Bashir, A. Q. Gill, and G. Beydoun, "A Reference Architecture for IoT-Enabled Smart Buildings," *SN Computer Science*, vol. 3, no. 6, p. 493, 2022