Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)
Vol. 9, No. 3, September 2023, pp. 549-557
ISSN: 2338-3070, DOI: 10.26555/jiteki.v9i3.26602

Design and Implementation of IoT-Based Burglary Detection System

Mokhalad Mahdi Jassem [1], Mohammed I. Al-Nouman [2]
[1] Department of Systems Engineering, College of Information Engineering, Al-Nahrain University, Jadriya, Baghdad,Iraq
[2] Department of Information and Communications Engineering, College of Information Engineering, Al-Nahrain University, Jadriya, Baghdad,Iraq

ARTICLE INFO

Article history:

Received June 04, 2023
Revised July 09, 2023
Published July 11, 2023

Keywords:

Camera;
Fingerprint;
IoT;
Raspberry Pi;
Security System

ABSTRACT

This paper aims to design and implement an IoT-based anti-theft security system. The system uses fingerprint recognition technology to grant access to a building only if the fingerprint matches the stored data. In case of unauthorized access attempts, the system captures a photo of the person and sends an immediate alert to the homeowner via the Telegram API. The proposed paper methodology involves analyzing existing systems, identifying research gaps, and developing a generally implementable framework. The proposed system is implemented using Raspberry Pi as the main control unit and incorporates components like the R305 Fingerprint Recognition Sensor, Camera Pi for video surveillance, and additional hardware for door control and sensor integration. Through practical testing, the implemented system demonstrates reliable burglary detection and notification capabilities, enhancing home or building security. Finally, the obtained research results offer valuable insights for future developments in anti-theft security systems.

Corresponding Author:

Mokhalad Mahdi Jassem, Al-Nahrain University, College of Information Engineering, Baghdad, IRAQ
Email: mokhalad.11.mahde@gmail.com

1. INTRODUCTION

Smart homes refer to residential spaces that are equipped with various interconnected devices and systems that enable automation, control, and monitoring of household functions and appliances, as shown in Fig. 1. These intelligent technologies allow homeowners to manage and optimize their living environment remotely or through voice commands. Smart homes typically incorporate devices such as smart thermostats, lighting systems, security cameras, door locks, and home entertainment systems that can be interconnected and controlled through a centralized hub or smartphone application. This integration provides convenience, energy efficiency, enhanced security, and the ability to customize and personalize the home environment according to individual preferences. Smart homes are revolutionizing the way we interact with our living spaces, offering greater comfort, efficiency, and peace of mind [1]-[8].

The security of smart homes is a critical aspect of their implementation. With the increasing number of interconnected devices and systems, it becomes crucial to ensure that the data and privacy of homeowners are protected. Smart homes face potential vulnerabilities, including unauthorized access to devices, hacking attempts, and data breaches. To mitigate these risks, robust security measures must be implemented, such as strong authentication mechanisms, encrypted communication protocols, regular software updates, and secure network configurations. Additionally, homeowners should follow best practices like using unique and strong passwords, enabling two-factor authentication, and being cautious while granting access to third-party applications. Continuous monitoring and surveillance systems can also help detect and respond to any security breaches promptly. By prioritizing security measures, smart homes can provide homeowners with peace of mind, knowing that their living spaces are protected from potential threats [9]-[12].

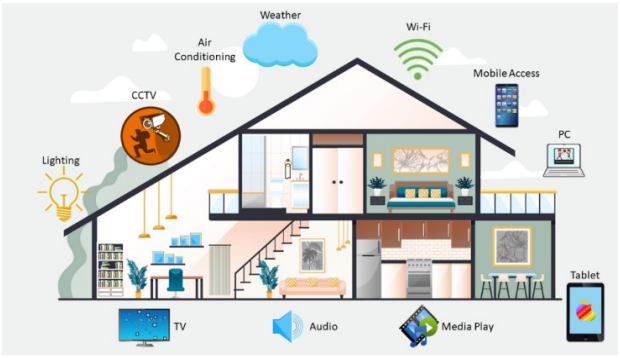

Fig. 1. Applications of smart homes.

Internet of Things (IoT) based security is crucial for protecting smart homes and their interconnected devices. With the IoT technology, various devices and systems in a smart home can communicate and share data, enhancing convenience and automation. However, this interconnectedness also introduces potential vulnerabilities that can be exploited by malicious actors. IoT-based security focuses on implementing measures to secure these devices and the communication networks they rely on. This includes measures such as robust authentication and authorization protocols, encryption of data transmission, regular software updates, and monitoring for any suspicious activity. Additionally, implementing firewalls, intrusion detection systems, and secure gateways can help protect against external threats. By prioritizing IoT-based security, smart homes can ensure that the benefits of interconnected devices are maximized while minimizing the risks associated with unauthorized access, data breaches, and privacy concerns [13]-[18].

The IoT structure comprises a network of interconnected devices, sensors, and systems that communicate and exchange data. It is a complex ecosystem where everyday objects, such as appliances, vehicles, and even clothing, are embedded with sensors, software, and connectivity capabilities. These devices gather and transmit data over the internet, allowing for seamless integration and automation. The IoT structure typically includes three main components: the devices themselves, the network infrastructure that enables communication, and the cloud-based platforms or applications that process and analyze the collected data, as shown in Fig. 2. This interconnected structure enables real-time monitoring, remote control, and data-driven decision-making. With the IoT structure, businesses and individuals can harness the power of connectivity to optimize processes, enhance efficiency, and create new opportunities across various industries [19]-[25].

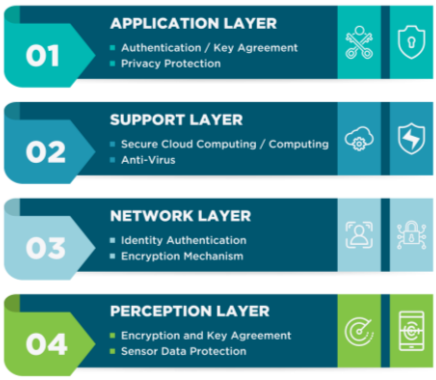

Fig. 2. Structure of IoT.

The research contribution in this work can be summarized as the design and implementation of a secure and efficient system aimed at protecting homes as well as other institutions from the risk of theft. The proposed system is based on two principal approaches: the first one utilizes fingerprint technology, while the second one relies on cameras integrated with the Telegram app. When an attempted theft or tampering occurs, the camera captures an image of the intruder and sends it to the homeowner via Telegram for security purposes.

2. UTILIZED HARDWARE

This part of the paper shows a brief introduction regarding the utilized hardware such as Raspberry Pi 3, Fingerprint module, and Camera.

2.1. Raspberry Pi

The Raspberry Pi 3 Model B is a single-board computer developed by the Raspberry Pi Foundation. It features a quad-core ARM Cortex-A53 processor running at 1.2 GHz and 1GB of RAM, providing improved performance for multitasking and responsiveness. One notable addition is the built-in Wi-Fi and Bluetooth capabilities, eliminating the need for external dongles. It includes a 10/100 Ethernet port, four USB 2.0 ports, HDMI and audio outputs, and a 40-pin GPIO header for connecting external devices. The Raspberry Pi 3 Model B uses a microSD card for storage and is widely used in various applications, including home automation, robotics, and educational projects, Fig. 3 illustrates the Raspberry Pi 3 kit [26]-[30].

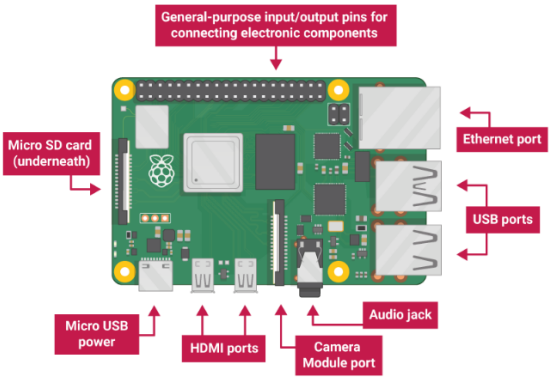

Fig. 3. Architecture of Raspberry Pi 3 kit.

2.2. Raspberry Pi Camera Module 2

The Raspberry Pi Camera Module 2 is a compact and lightweight camera module designed specifically for Raspberry Pi boards. It connects directly to the Raspberry Pi's CSI port, offering a hassle-free setup. This high-quality camera module supports up to 8-megapixel still images and 1080p video recording, thanks to its fixed-focus lens. It provides a versatile range of features, including adjustable focus, exposure, white balance, and image effects. The module also supports different capture modes like burst mode and time-lapse and can be programmed using Python or other languages for image capture or video recording. By integrating the Raspberry Pi Camera Module 2, users can effortlessly add camera functionality to their Raspberry Pi projects. It finds common applications in surveillance systems, video streaming, computer vision projects, and more. With its compact size and compatibility with Raspberry Pi boards, this camera module is a popular choice for capturing high-quality media in various projects; Fig. 4 shows the Raspberry Pi Camera Module V2 [31]-[35].

Fig. 4. Raspberry Pi Camera Module V2.

2.3. Fingerprint Module

The R305 Fingerprint Recognition Sensor is a biometric sensor used to capture and identify fingerprints. It employs optical scanning technology to capture high-resolution fingerprint images and extract distinctive features for authentication purposes. With its advanced algorithm, it can swiftly and accurately verify an individual's identity based on their fingerprint. The sensor includes features such as fake fingerprint detection and support for storing a large number of templates. It can be effortlessly integrated into diverse projects and systems through standard communication protocols. In summary, the R305 Fingerprint Recognition Sensor offers a dependable and secure solution for fingerprint-based identification and authentication. Fig. 5 shows R305 fingerprint module [36], [37].

Fig. 5. R305 fingerprint module.

2.4. Servo Motor

The SG90 servo is a small, lightweight, and affordable servo motor that finds widespread use in robotics, RC (remote control) vehicles, and various electronic projects. It is a compact motor capable of rotating within a specific range, typically around 180 degrees. The SG90 servo is renowned for its precise positioning and relatively high torque considering its size. It operates by responding to a control signal, usually a PWM (Pulse Width Modulation) signal, which determines the desired position of the servo shaft. Based on the control signal, the servo motor adjusts its position, allowing for precise control over angular movement. The SG90 servo is user-friendly and compatible with a variety of microcontrollers and development boards. It is commonly employed in tasks such as controlling robotic arms and steering mechanisms. Fig. 6 shows a micro servo motor with a pins configuration [38], [39].

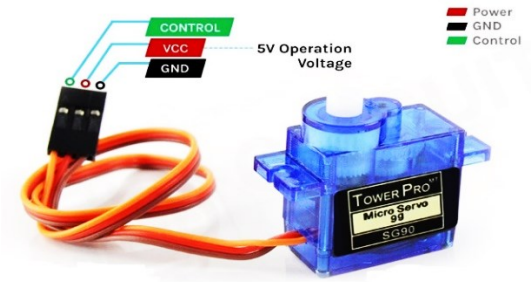

Fig. 6. Micro servo motor.

2.5. Magnetic lock Sensor

The magnetic door sensor is a vital component of your anti-theft system, specially designed to detect the opening and closing of doors or windows. It comprises two parts: a magnet and a sensor, as shown in Fig. 7. When the door or window is closed, the magnet is in close proximity to the sensor, generating a magnetic field. If the door or window is opened, the magnet moves away from the sensor, interrupting the magnetic field and initiating an alert signal. This sensor plays a crucial role in detecting unauthorized access and activating the security system to prevent burglaries or break-ins [40], [41].

Fig. 7. Magnetic lock sensor.

3. SYSTEM DESIGN AND IMPLEMENTATION

This section of the paper discusses the study area and methodology utilized in developing the anti-theft system. The proposed system incorporates various sensors, such as motion sensors and door sensors, to detect unauthorized access attempts. The system utilizes a fingerprint recognition module to grant access solely to authorized individuals. If an unauthorized person attempts to access the building, the system captures a photo

of them and sends an alert to the administrator via the Telegram API. Furthermore, we will elucidate the algorithm employed in the anti-theft system process. This chapter offers a thorough analysis of the implemented IoT-based burglary detection system. The chapter then proceeds with a detailed examination of the obtained results. Lastly, the chapter concludes by emphasizing the significance of the obtained results and their implications for future advancements in anti-theft and security systems. Overall, this chapter serves as a comprehensive overview of the system's implementation, providing valuable insights into its performance, reliability, and potential for further development.

3.1. Proposed Methodology

The methodology that is used to create the proposed IoT-based burglary detection system can be summarized as follows:

a) System Design: The system architecture and components are designed based on the requirements and objectives of the project. The integration of the Raspberry Pi, Camira Pi, fingerprint recognition sensor, servo, and other tools is carefully planned.
b) Hardware Setup: The hardware components, including the Raspberry Pi, Camira Pi, fingerprint recognition sensor, servo, buzzer, magnetic door sensors, Pi UPS power, breadboard power supply, and 9V battery, are connected and configured according to their respective specifications.
c) Software Development: Software programs and scripts are developed to enable communication between the hardware components, perform fingerprint recognition, capture video footage, detect unauthorized access, and send real-time notifications.
d) Testing and Validation: The system is tested extensively to ensure its functionality, reliability, and accuracy. Various scenarios and situations are simulated to evaluate the system's performance and its ability to detect and respond to unauthorized access attempts.
e) Implementation: The fully functional system is implemented in a residential setting, where it is deployed to monitor the premises and provide real-time burglary detection and notification capabilities.

By following this methodology and utilizing the specified tools and components, the IoT-based burglary detection system has been successfully developed and implemented, as presented in the next sections.

3.2. Proposed System Architecture

The system architecture of the proposed anti-theft system consists of four main components: the fingerprint scanner, the Raspberry Pi, the camera module, and the Telegram API. The fingerprint scanner module is responsible for scanning the fingerprint of an individual seeking access to the building. It is connected to the Raspberry Pi, which acts as the main processing unit of the system. The Raspberry Pi controls the flow of data between the various components of the system.The camera module is utilized to capture images of individuals attempting to gain unauthorized access to the building. It is connected to the Raspberry Pi and is triggered when the fingerprint scanner module detects an unauthorized individual. The Telegram API is employed to send alerts to the building owner in case of unauthorized access. The Raspberry Pi is connected to the Telegram API and sends a notification to the owner's phone when an unauthorized individual is detected. The proposed system is designed to be adaptable and scalable, allowing customization to meet the specific needs of different buildings. It can also be easily integrated with other security systems. The use of open-source technologies such as Raspberry Pi and the Telegram API makes the system cost-effective and accessible to a broader range of users.

3.3. System Implementation

The implementation of the anti-theft and security system involved integrating hardware and software components to achieve the desired functionality. The hardware components utilized in the implementation included a Raspberry Pi microcomputer, a fingerprint sensor module, a camera module, and a Wi-Fi module. The software components encompassed the Python programming language, OpenCV library for image processing, Flask framework for web development, and the Telegram API for real-time notifications.The fingerprint sensor module captured fingerprints and stored them in a database for verification purposes. The camera module captured images of any unauthorized access attempts, which were then processed using OpenCV to detect human faces and trigger the system's alert function. The Raspberry Pi microcomputer acted as the central processing unit, receiving inputs from the sensors and processing them to trigger appropriate outputs. The Wi-Fi module facilitated the system in sending real-time notifications to the house owner/member through the Telegram API. The system was implemented using the Model-View-Controller (MVC) architecture, with the Raspberry Pi as the controller, the fingerprint sensor and camera modules as the models, and the Flask framework as the view. The MVC architecture ensured the separation of concerns and modularity

of the system components, simplifying maintenance and scalability. The implementation of the anti-theft and security system progressed in phases, with each phase involving testing and validation of the system's functionality. The first phase entailed implementing the fingerprint sensor module and the database management system. The second phase involved implementing the camera module and the OpenCV image processing library. The third phase focused on integrating the hardware components and the Flask framework. The final phase encompassed testing and validating the entire system, including real-world scenarios. The implementation of the anti-theft and security system was successful, as it effectively detected and prevented unauthorized access attempts in real-time. The system's modular architecture facilitated ease of maintenance and scalability, while the use of open-source software components made it cost-effective and customizable, Fig. 8 shows the implanted system.

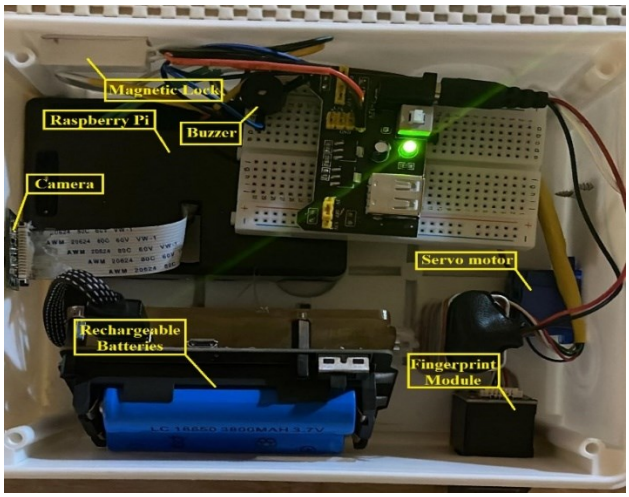

Fig. 8. Implanted prototype for the proposed system.

After completing the installation of the Raspberry Pi and ensuring its readiness for work, including photo capturing and face recognition capabilities, the next step is to create a Telegram bot. This bot will enable us to receive pictures from the Raspberry Pi for further processing. To create the bot, we can utilize a service like BotFather, which offers a user-friendly interface for creating and managing Telegram bots. Using BotFather, we generate a unique token for our bot, which serves as its identification. We copy the generated token and paste it into the appropriate location within our code. This token will be utilized to establish communication between the Raspberry Pi and the Telegram platform. By creating and configuring the Telegram bot, we enable the Raspberry Pi to send pictures and relevant notifications to the designated Telegram account. This facilitates real-time monitoring and alerts for security purposes. Once the Telegram bot is set up, the Raspberry Pi is ready to send photos to Telegram. Whereas the necessary library for interacting with the Telegram bot has been installed, and the token has been included in the code.

There are two separate code files for different functionalities. The first file is responsible for running the face recognition process in the background. It captures images from the camera and detects faces in those images. This file operates continuously to identify faces and perform subsequent actions. The second file focuses on fingerprint recognition. It serves as the user interface, allowing users to input their fingerprints. If a matching fingerprint is found, the system will grant access by opening the door.

Within the fingerprint recognition file, the user will come across four options displayed on the screen. To initiate the fingerprint enrollment process, select the option labeled "enroll." The program will prompt user to enter a name and position his hand accordingly. Once user ready, it will capture an image of his hand.Next, the program will instruct user to place his finger onto the fingerprint sensor. It will continue capturing images of his fingerprint until it obtains an accurate representation. The captured fingerprint image will be saved on the desktop, as indicated in Fig. 9, and the fingerprint data will be stored within the fingerprint device for future recognition purposes.

In the second scenario, when selecting the "find" option within the fingerprint recognition file, the program will prompt the user to remove his finger from the sensor. Upon doing so, it will proceed to verify the captured fingerprint against the stored fingerprint data. If a match is found, indicating that the fingerprint belongs to an authorized individual, the program will proceed to open the door and display two images. The first image will show the person who enrolled in the fingerprint, providing visual confirmation of their identity.

The second image will be displayed alongside the person's name, indicating a successful match between the fingerprint and the enrolled user.

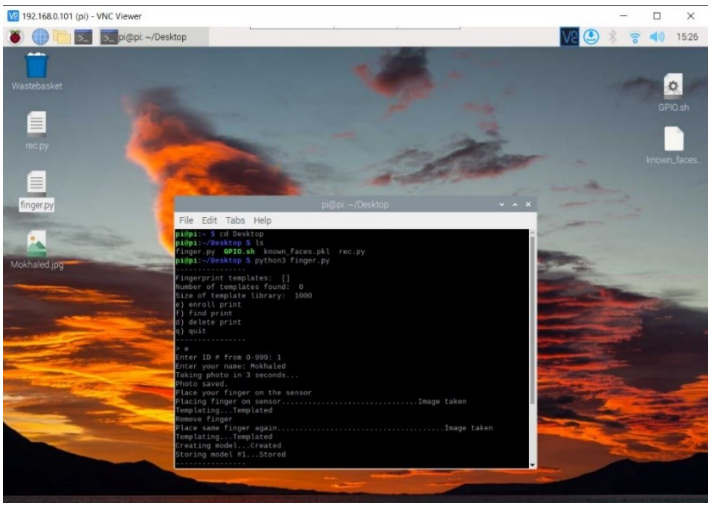

Fig. 9. Enrollment for fingerprint.

In the second program, the face recognition tool processes the captured image to detect and identify faces, as shown in Fig. 10. When a face is successfully recognized, the program retrieves the corresponding name associated with that face from the database. Subsequently, the program utilizes the Telegram bot to send a message containing the person's name to a specified Telegram account or group. This notification or alert informs the user that a face has been detected and recognized. By integrating the face recognition tool with the Telegram bot, the system enables real-time notifications and offers the capability to remotely monitor and receive updates on recognized individuals.

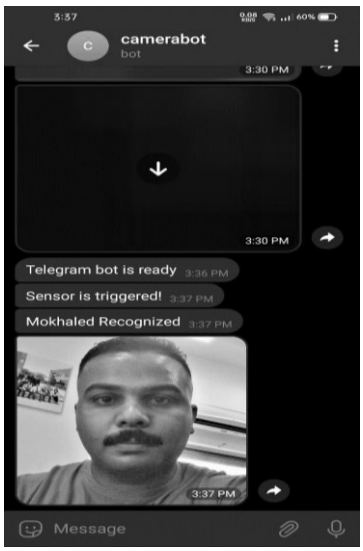

Fig. 10. Telegram Camera Bot response.

4. CONCLUSION

In conclusion, the IoT-based burglary detection system presented in this paper has effectively addressed the limitations of traditional security systems and provided a reliable and efficient solution to enhance home security and prevent burglaries. The system utilizes fingerprint recognition technology to grant access to the building only when the person's fingerprint matches the one stored in the system. In the event of an unauthorized access attempt, the system captures a photo of the person and sends an alert to the administrator using a Telegram API-programmed interface. The implementation and testing of the system have demonstrated its effectiveness in detecting unauthorized access and providing real-time alerts to homeowners/members. Moreover, the system is designed to be easily deployable, customizable, and affordable for average

homeowners. However, certain limitations and challenges were identified during the implementation phase, such as the requirement for a stable internet connection and potential issues with false alarms. These challenges can be addressed in future work by incorporating additional sensors and detectors and refining the algorithm employed in the anti-theft system process. Overall, this project has made a valuable contribution to the field of home security systems by developing a reliable and efficient IoT-based solution. Future work can focus on enhancing the system's accuracy and reliability, integrating it with other IoT devices, and exploring its applicability in various settings, including commercial buildings and public areas.

REFERENCES

[1] A. Sahrab and H. M. Marhoon, "Design and fabrication of a low-cost system for Smart Home Applications," *Journal of Robotics and Control (JRC)*, vol. 3, no. 4, pp. 409–414, 2022, https://doi.org/10.18196/jrc.v3i4.15413.

[2] L. Babangida, T. Perumal, N. Mustapha and R. Yaakob, "Internet of Things (IoT) Based Activity Recognition Strategies in Smart Homes: A Review," in *IEEE Sensors Journal*, vol. 22, no. 9, pp. 8327-8336, 2022, https://doi.org/10.1109/JSEN.2022.3161797.

[3] P. K. Sattaru, K. V. Burugula, R. Channagiri and S. Kavitha, "Smart Home Security System using IoT and ESP8266," *5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 469-474, 2023, https://doi.org/10.1109/ICSSIT55814.2023.10061059.

[4] W. Li, T. Logenthiran, V. -T. Phan and W. L. Woo, "A Novel Smart Energy Theft System (SETS) for IoT-Based Smart Home," in *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5531-5539, 2019, https://doi.org/10.1109/JIOT.2019.2903281.

[5] V. Bianchi, M. Bassoli, G. Lombardo, P. Fornacciari, M. Mordonini and I. De Munari, "IoT Wearable Sensor and Deep Learning: An Integrated Approach for Personalized Human Activity Recognition in a Smart Home Environment," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8553-8562, 2019, https://doi.org/10.1109/JIOT.2019.2920283.

[6] Q. I. Sarhan, "Arduino Based Smart Home Warning System," *IEEE 6th International Conference on Control Science and Systems Engineering (ICCSSE)*, pp. 201-206, 2020, https://doi.org/10.1109/ICCSSE50399.2020.9171939.

[7] S. S. Tippannavar, S. N and P. K. M. S, "Smart Home Automation Implemented using LabVIEW and Arduino," *International Conference on Electronics and Renewable Systems (ICEARS)*, pp. 644-649, 2022, https://doi.org/10.1109/ICEARS53579.2022.9752265.

[8] B. Santhikiran, L. Nagaraju, S. Abdul Sattar, D. Bharath Chandra, and Y. Jayasankar, "Design and Implementation of Smart Home System Based on IoT and Esprainmaker," *International Transactions on Electrical Engineering and Computer Science*, vol. 2, no. 2, pp. 70-79, 2023, https://www.iteecs.com/index.php/iteecs/article/view/45.

[9] R. Sarmah, M. Bhuyan and M. H. Bhuyan, "SURE-H: A Secure IoT Enabled Smart Home System," *IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 59-63, 2019, https://doi.org/10.1109/WF-IoT.2019.8767229.

[10] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir and M. Imran, "Investigating Smart Home Security: Is Blockchain the Answer?," in *IEEE Access*, vol. 8, pp. 117802-117816, 2020, https://doi.org/10.1109/ACCESS.2020.3004662.

[11] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042-9053, 2019, https://doi.org/10.1109/JIOT.2019.2926365.

[12] H. M. Marhoon, M. I. Mahdi, E. Dh. Hussein, and A. R. Ibrahim, "Designing and implementing applications of Smart Home Appliances," *Modern Applied Science*, vol. 12, no. 12, pp. 8–17, 2018, https://doi.org/10.5539/mas.v12n12p8.

[13] D. Rani, N. S. Gill, P. Gulia, F. Arena and G. Pau, "Design of an Intrusion Detection Model for IoT-Enabled Smart Home," in *IEEE Access*, vol. 11, pp. 52509-52526, 2023, https://doi.org/10.1109/ACCESS.2023.3276863 =,

[14] A. H. . Mukalaf, H. M. . Marhoon, I. . Suwarno, and A. . Ma'arif, "Design and Manufacturing of Smart Car Security System with IoT-Based Real-Time Tracking," *Int J Intell Syst Appl Eng*, vol. 11, no. 6s, pp. 745-752, 2023, https://www.ijisae.org/index.php/IJISAE/article/view/2909.

[15] I. Antzoulis, M. M. Chowdhury and S. Latiff, "IoT Security for Smart Home: Issues and Solutions," *IEEE International Conference on Electro Information Technology (eIT)*, pp. 1-7, 2022, https://doi.org/10.1109/eIT53891.2022.9813914.

[16] M. Murad, O. Bayat, and H. M. Marhoon, "Design and implementation of a smart home system with two levels of security based on IOT Technology," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 21, no. 1, pp. 546–557, 2021, https://doi.org/10.11591/ijeecs.v21.i1.pp546-557.

[17] Q. I. Sarhan, "Arduino Based Smart Home Warning System," *IEEE 6th International Conference on Control Science and Systems Engineering (ICCSSE)*, pp. 201-206, 2020, https://doi.org/10.1109/ICCSSE50399.2020.9171939.

[18] P. K. Sattaru, K. V. Burugula, R. Channagiri and S. Kavitha, "Smart Home Security System using IoT and ESP8266," *5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 469-474, 2023, https://doi.org/10.1109/ICCSSE50399.2020.9171939.

[19] Q. Li, Q. Zhang, H. Huang, W. Zhang, W. Chen and H. Wang, "Secure, Efficient, and Weighted Access Control for Cloud-Assisted Industrial IoT," in *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 16917-16927, 2022, https://doi.org/10.1109/JIOT.2022.3146197.

[20] S. E. Mathe, A. C. Pamarthy, H. K. Kondaveeti and S. Vappangi, "A Review on Raspberry Pi and its Robotic Applications," *2nd International Conference on Artificial Intelligence and Signal Processing (AISP)*, pp. 1-6, 2022, https://doi.org/10.1109/AISP53593.2022.9760590.

[21] V. Kamath and R. A., "Performance analysis of the pre-trained EfficientDet for real-time object detection on Raspberry Pi," *International Conference on Circuits, Controls and Communications (CCUBE)*, vol. 11, no. 1, pp. 834–838, 2021, https://doi.org/10.1109/CCUBE53681.2021.9702741.

[22] P. Daponte, F. Lamonaca, F. Picariello, L. De Vito, G. Mazzilli and I. Tudosa, "A Survey of Measurement Applications Based on IoT," *Workshop on Metrology for Industry 4.0 and IoT*, pp. 1-6, 2018, https://doi.org/10.1109/METROI4.2018.8428335.

[23] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," in *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16-32, 2020, https://doi.org/10.1109/JIOT.2019.2948888.

[24] Z. Wang *et al*., "A Survey on IoT-Enabled Home Automation Systems: Attacks and Defenses," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2292-2328, 2022, https://doi.org/10.1109/COMST.2022.3201557.

[25] D. Pavithra and R. Balakrishnan, "IoT based monitoring and control system for home automation," *Global Conference on Communication Technologies (GCCT)*, pp. 169-173, 2015, https://doi.org/10.1109/GCCT.2015.7342646.

[26] Z. Zhu *et al*., "CBASH: A CareBot-Assisted Smart Home System Architecture to Support Aging-in-Place," in *IEEE Access*, vol. 11, pp. 33542-33553, 2023, https://doi.org/10.1109/ACCESS.2023.3264272.

[27] I. Mashal, A. Shuhaiber, and A. wael AL-Khatib, "User acceptance and adoption of Smart Homes: A Decade Long Systematic Literature Review," *International Journal of Data and Network Science*, vol. 7, no. 2, pp. 533–552, 2023, https://doi.org/10.5267/j.ijdns.2023.3.017.

[28] V. A. Orfanos, S. D. Kaminaris, P. Papageorgas, D. Piromalis, and D. Kandris, "A comprehensive review of IOT networking technologies for Smart Home Automation Applications," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, pp. 30–38, 2023, https://doi.org/10.3390/jsan12020030.

[29] B. Garn, D. -P. Schreiber, D. E. Simos, R. Kuhn, J. Voas and R. Kacker, "Summary of Combinatorial methods for testing Internet of Things smart home systems," *IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pp. 266-267, 2023, https://doi.org/10.1109/ICSTW58534.2023.00054.

[30] K. S, A. R, M. V. Cruz, L. Chen, A. V. J. L and R. V. S, "A Systematic Analysis on Raspberry Pi Prototyping: Uses, Challenges, Benefits, and Drawbacks," in *IEEE Internet of Things Journal*, p. 1, 2023, https://doi.org/10.1109/JIOT.2023.3262942.

[31] S. E. Mathe, A. C. Pamarthy, H. K. Kondaveeti and S. Vappangi, "A Review on Raspberry Pi and its Robotic Applications," *2nd International Conference on Artificial Intelligence and Signal Processing (AISP)*, pp. 1-6, 2022, https://doi.org/10.1109/AISP53593.2022.9760590.

[32] N. I. binti Rasidi, O. Ismael Al-Sanjary, M. Y. Kashmola and K. Loo Teow Aik, "Development on Autonomous Object Tracker Robot using Raspberry Pi," *IEEE 10th Conference on Systems, Process & Control (ICSPC)*, pp. 29-33, 2022, https://doi.org/10.1109/ICSPC55597.2022.10001745.

[33] S. S. I, R. Ramli, M. A. Azri, M. Aliff and Z. Mohammad, "Raspberry Pi Based Driver Drowsiness Detection System Using Convolutional Neural Network (CNN)," *IEEE 18th International Colloquium on Signal Processing & Applications (CSPA)*, pp. 30-34, 2022, https://doi.org/10.1109/CSPA55076.2022.9781879.

[34] A. Baobaid, M. Meribout, V. K. Tiwari and J. P. Pena, "Hardware Accelerators for Real-Time Face Recognition: A Survey," in *IEEE Access*, vol. 10, pp. 83723-83739, 2022, https://doi.org/10.1109/ACCESS.2022.3194915.

[35] F. Wang, R. Zheng, P. Li, H. Song, D. Du and J. Sun, "Face recognition on Raspberry Pi based on MobileNetV2," *International Symposium on Artificial Intelligence and its Application on Media (ISAIAM)*, pp. 116-120, 2021, https://doi.org/10.1109/ISAIAM53259.2021.00031.

[36] L. Kamelia, E. A. D. Hamidi, W. Darmalaksana and A. Nugraha, "Real-Time Online Attendance System Based on Fingerprint and GPS in the Smartphone," *4th International Conference on Wireless and Telematics (ICWT)*, pp. 1-4, 2018, https://doi.org/10.1109/ICWT.2018.8527837.

[37] M. Rukhiran, S. Wong-In and P. Netinant, "IoT-Based Biometric Recognition Systems in Education for Identity Verification Services: Quality Assessment Approach," in *IEEE Access*, vol. 11, pp. 22767-22787, 2023, https://doi.org/10.1109/ACCESS.2023.3253024.

[38] I. A. Taha and H. M. Marhoon, "Implementation of controlled robot for fire detection and extinguish to closed areas based on Arduino," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 16, no. 2, pp. 654-664, 2018, https://doi.org/10.12928/telkomnika.v16i2.8197.

[39] A. Murad, O. Bayat, and H. M. Marhoon, "Implementation of rover tank firefighting robot for closed areas based on Arduino microcontroller," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 56–63, 2021, https://doi.org/10.11591/ijeecs.v21.i1.pp56-63.

[40] D. -I. Gota, A. Puscasiu, A. Fanca, L. Miclea and H. Valean, "Smart home automation system using Arduino microcontrollers," *IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)*, pp. 1-7, 2020, https://doi.org/10.1109/AQTR49680.2020.9129989.

[41] A. S. Ibrahim, A. M. Abbas, A. M. A. Hassan, W. M. F. Abdel-Rehim, A. Emam and S. Mohsen, "Design and Implementation of a Pilot Model for IoT Smart Home Networks," in *IEEE Access*, vol. 11, pp. 59701-59728, 2023, https://doi.org/10.1109/ACCESS.2023.3282095.