International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Shield Sight: Advanced Frith System

Ankur Chopde[1], Radhika Muley[2], Dr. S. B. Dhoot[3]

[1,2]Polytechnic Student, Electronics and Telecommunication, Government Polytechnic of Chh. Sambhajinagar
[3]Head of Department, Electronics and Telecommunication, Government Polytechnic of Chh. Sambhajinagar

Abstract
Security is an utmost requirement for domestic, commercial, and industrial complexes. Conventional security systems rely only on primitive monitoring without real-time threat detection and response. Shield Sight Advanced Frith System aims to overcome these limitations through the integration of intelligent, multi-level security technologies that conduct real-time observation, automatic identification, verification, and instant warning messages. The system has a Raspberry Pi 4 as the central processing unit, managing the processing of data, authentication, and communication. The system has sensors like PIR motion detectors, camera modules, and biometric authentication to include an adaptive security component. Remote administration, user administration of access, and real-time event monitoring is provided through a web interface. The project becomes more secure due to the introduction of AI-fueled threat analysis, biometric authentication, and automated access control and incorporating it into many security-sensitive contexts
.

Keywords: Raspberry Pi 4, face recognition, intrusion detection, website, alert, G-Mail, tampering detection.

1. INTRODUCTION

Security is essential for the protection of homes, offices, and business sites. The traditional security systems are not intelligent enough to identify threats in real-time and react accordingly, hence in effect failing to prevent unauthorized access and potential threats effectively. Shield Sight Advanced Frith System overcomes these shortcomings by offering an intelligent, multi-level security solution that ensures real-time monitoring, instant alerts, and efficient management of users.

In comparison to the conventional systems, which employ simple monitoring, the system uses automated detection, authentication, and alerting features to provide more security. The system provides multi-layer authentication to prevent unauthorized access and has a separate website for simple database management, where user access rights can easily be controlled. The system can instant alerts to notify users of any threat happening to system.

At the centre of this system is a high-tech processing core that efficiently performs detection, authentication, and communications functions. In delivering real-time security monitoring and automation, it reduces human interference to the minimum while offering maximum safety and reliability. The system is also very user-friendly and scalable, thus being suitable in a wide range of applications from home security to high-security business settings.

In its effective structure and implementation, the project attempts to redefine norms of security by a wise

and active approach towards solving modern security issues.

2. LITERATURE REVIEW

The paper by Raju A Nadaf et al. suggests an intelligent security system for human intrusion detection with various detection methods to ensure accuracy and efficiency. With the integration of better recognition techniques, the system ensures enhanced performance with real-time detection and response. The paper defines the issue of getting clear images for verification and highlights the necessity of optimized image processing to ensure reliability in detection. Also, the work underscores proper utilization and programming of resources, specifically in embedded platform-based systems, in order to provide smooth-running performance and processing delay reduction. The result illustrates that the usage of optimized models in detection results in high system responsiveness, so it is efficient to use with high accuracy as well as quick detection of threats for real-time security applications. [1]

Internet of Things (IoT) provides facilities of smooth intercommunication among objects, improving security and automation. Face recognition technology is a key component in monitoring and access control systems and requires efficient and cost-effective solutions. In this context, the study by Arti Kate et al. investigates the implementation of a face recognition system based on traditional approaches using a Raspberry Pi. It takes photos upon guest arrival, captures timestamp, and offers real-time view via a web interface. It utilizes IoT to support remote access, real-time video streaming, and instant notifications for improved security. The system is made deployable easily and automated so that it becomes a viable option for visitor monitoring and access control. [2]

Video surveillance is currently an integral part in security and guarding in industries with real-time tracking of assets, people, and environments. This paper by Mohanad Abdulhamid et al. presents the use of an embedded real-time monitoring system based on the Raspberry Pi single-board computer (SBC) for intruder detection to enhance security through embedded control and alarm functions is introduced. The emerging system combines web applications with cameras and motion sensors to offer remote monitoring. The Raspberry Pi powers and manages motion sensors and cameras, offering real-time video streaming and recording for future use. The system also offers real-time intrusion detection, snaps photos, and alerts the owner via a wireless module. Such low-cost, yet high-efficiency security system can be easily installed and offers benefits in remote security monitoring. The article also presents motion detection and object tracking with image processing, utilizing pixel thresholding methods in more sophisticated surveillance applications. Real-time video streams illustrate object recognition and object tracking in motion, and how crucial the technology is for contemporary security applications. [3]

Security has, in the contemporary era, become an integral part of life, providing protection for the home and members of the family. In technological development, the Internet of Things (IoT) has significantly contributed to security software by allowing interconnected devices to effectively communicate with each other. Human observation is used in traditional surveillance systems, which is not effective and slow. This paper by Dr. Nagalakshmi Venugopal et al. demonstrates an IoT smart security system that uses computer vision for detection and surveillance. A Raspberry Pi 3 with an exxternal camera acts as the processing unit that photographs and identifies individuals. The Raspberry Pi also contains an ultrasonic sensor, which detects intrusions and gives warnings with picture taking. The images are delivered to the user in real-time via a wireless application, enabling real-time monitoring and alert. The employed system in this case is an efficient, economical, and smart security system that may be installed in contemporary homes and other vulnerable locations. By combining IoT with computer vision, the system is able to increase

monitoring and provide users with real-time alarms and visual proofs of security incidents.[4]

With each passing day, technology moves a step ahead and offers new alternatives to displace current systems, especially security systems. This paper by Shital A. Patil and Deepak B.Kadam presents how a self-powered wireless security camera system can be used for far-end monitoring. The aim here is to implement a network such that image forwarding and receiving occur smoothly from the camera nodes to a base station. As automobile offenses, i.e., automobile theft and vandalism, are becoming ever more problematic, wired security systems have been shown to be too expensive and ineffectual based on the infrastructure requirement. Wireless security cameras present an economic yet effective solution without the need for costly wiring and allowing real-time observation. The system employs Raspberry Pi as a processing device in order to use web cameras to capture images and view remotely. In contrast to traditional surveillance systems based on skilled personnel viewing video, such an installation provides independent viewing with less human intervention and ultimate security. Snapshots taken and continuous feeds are sent to a specified monitoring station, where users can view video in real-time or access saved evidence as and when required. The convenience of installation and economical benefits render wireless security camera systems more commonly applied for commercial as well as residential applications. Their flexibility also makes them easy to install at various points such as apartments without requiring the landlords' approval. With the solution of the shortcomings of conventional security arrangements, the system offers a new, scalable, and effective surveillance solution for contemporary security requirements. [5]

With surveillance systems, face recognition enhances security and automation and is an inevitable tool for various uses such as school, office, and secure facility attendance monitoring. Traditional methods such as RFID and fingerprint-based attendance systems are succeeded by weaknesses such as susceptibility to fraud, ineffectiveness, and susceptibility to external influences. Face recognition offers a contactless and secure system that offers real-time identification with minimal human involvement. This paper by Dhanshri Mali et al. suggests a facial-based intelligent monitoring system to implement automatic attendance with improved accuracy and ease of use. High-definition cameras, advanced algorithms, and mobile remote monitoring and control for improved system performance are emphasized in future development. [6]

Surveillance and security are commonplace in today's age in domestic and commercial settings. The present work by Mekecha Banchigize Bazezew suggests an intelligent face recognition-based security system that includes motion detection and a variety of sensors for intrusion detection and real-time monitoring. Operating on Raspberry Pi as the processing platform, the system uses microwave radar, infrared imaging, magnetic field detection, and PIR sensors for enhanced detection accuracy for intruders and objects. The system alerts in real time through email, mobile app pop-ups, and an in-app application for long-distance monitoring and control. Featuring cost-effective and easy installation, this security system is a modern solution for deployment in offices, residences, labs, and security areas. It will be made more efficient by integrating future higher-level AI algorithms, high-def cameras, and cloud-based computing in the years to come. [7]

This paper by Md. Rakib Ahsan et al. presents a security and home automation system is suggested that uses the implementation of IoT technology to remotely monitor and manage domestic appliances for ease of use. The system uses a microcontroller assisted by Wi-Fi to develop a reliable and effective communication system, and the user is enabled to monitor devices through a web portal. It also features sensors for real-time security monitoring with alarm in case of unauthorized entry or dangerous incidents.

This is an economical, reliable, and scalable solution for upcoming home automation needs with low power consumption while ensuring maximum convenience. AI-based automation can be the answer in the future to achieve maximum efficiency and security. [8]

This paper by Abdu Subhan et al. introduces a home automation system with gas leak detection to promote security and safety. The system applies IoT-recommended sensors to monitor gas leaks in real time, triggering real-time alarms and automatic shutdown features to avoid any dangers. Smartphones provide continuous remote monitoring, granting homeowners further control and peace of mind. Although it faces challenges like sensor reliability, maintenance, and system complexity, AI advancements, machine learning, and IoT will enhance efficiency and reliability. The solution marks an important advancement towards smart, secure homes with fewer risks and overall increased security. [9]

This project by Bharti Chouhan et al. is home security with GSM-based communication integration for live monitoring and alarm systems. The system provides remote control of home appliances like geysers, air conditioners, fans, and lights, and gas leakage detection using wireless sensors. The system offers instant SMS notification to subscribed users in case of security violation or gas leakage, thereby facilitating timely response and preventive actions. The system, using GSM technology, gives a cost-effective and secure security and home automation solution with convenient control and protection wherever one happens to be anywhere in the world. [10]

The article by Keerthana Chandran introduces the application of a cutting-edge wireless video monitoring system over the Internet of Things (IoT) for improved security and real-time monitoring. The system combines high-definition video processing, network protocol optimization, and congestion control functions to provide data transmission with high efficiency and low latencies of packet losses. A multi-camera tracking system provides smooth monitoring of big spaces, enhancing coordination and accuracy of object detection. Apart from that, Bayesian-based event modeling technique improves data analysis and eliminates system redundancy. The proposed algorithm greatly improves video surveillance performance and provides a robust, scalable, and smart security solution for various applications. [11]

With the internet readily accessible almost anywhere, network security in the 21st century has been a concern to keep from unauthorized access. Intrusion Detection Systems (IDS) by Vikrant H. Modi and Ami A. Patel have an important function of detecting and thwarting security incursions. The following is a general overview of various types of IDS, which are signature-based and anomaly-based detection approaches and their weaknesses and strengths. It also touches on the history of IDS in today's day and age, within the scope of actual application and measuring devices such as the DARPA dataset. It is interested in how emerging techniques such as sensor fusion and behavior analysis can be utilized to enhance the performance of IDS for better safeguarding against cyber attacks. [12]

With advancements in technology at a very fast pace during the Internet of Things (IoT) age, smart electrical appliances are becoming a key element of contemporary home automation systems. The project by Mihir Upagade et al. presents an IoT-backed economically smart electrical device automation system powered by an ESP32 Wi-Fi module and a bespoke private web server. The system offers registered users remote monitoring and control of their electrical appliances for greater convenience and energy efficiency. Utilizing embedded systems and wireless communication, this solution would be an inexpensive and efficient method of converting typical electrical appliances to intelligent and networked appliances that can make domestic living smarter and more convenient. [13]

The rapid evolution of IoT technology has made possible sophisticated security monitoring systems with real-time surveillance and warning. The given project by Prof. Muzaffar Khan et al. illustrates low-cost

IoT-based smart security system with the use of a Raspberry Pi and camera module to detect movement and alert users through photographs, videos, and messages. Upon triggering an intruder, the system buffers and stores locally or in the cloud for ready access even when the network is down. FFmpeg integration with Pushbullet capabilities enhances user experience through mobile and web remote monitoring. The intelligent surveillance solution is appropriate for home, office, and high-security applications with an economical as well as a reliable solution to current security requirements. [14]

Security has become one of the key features of smart homes and offices over the last few years, leading to the evolution of intelligent surveillance systems. In this paper which is presented by SrushtiA. Nagtode et al., the authors propose the creation of a real-time facial recognition system on Raspberry Pi for protecting the system. The system utilizes a PIR sensor to sense motion, which triggers the Raspberry Pi camera to capture photos. The images are processed using computer vision techniques, i.e., Local Binary Pattern (LBP) for facial recognition. Upon detection, the system alerts and forwards images to a smartphone via an IoT-based Telegram application. The proposed system is low cost, efficient, and suitable for real-time applications. Experimental results prove its capability to provide secure access control with reduction of false alarms compared to traditional PIR-based or SMS alert systems. [15]

Previous research paper of this one named "An IoT Based Multipurpose Frith System: A Review" presents a review of a smart home security system that attempts to keep up with growing demands for efficient security systems due to increasing crime rates. The system employs a top-level model Raspberry Pi to provide multiple layers of verification, such as fingerprint recognition and live previewing of the cameras, and real-time detection of violence. It employs IoT and machine learning technology to keep a real-time surveillance and also provides notifications in case of intrusion or violent behavior through Gmail authentication. The key is that it has a facial recognition feature to clearly differentiate between authorized and unregistered users with fewer false alarms. It also provides an option for guest control with temporary admission of guests according to defined conditions. The moment an intrusion has been attempted, the system will automatically notify the owner through video and audio capturing of the breach, and the whole-sized yet budget-friendly security solution can then be installed at home or office. [16]

3. PROJECT OVERVIEW

Today's surveillance requires intelligence and automation in order to provide security, and intelligent systems must hence be incorporated for combining real-time monitoring, authentication, and threat response on a automated level. Traditional security solutions do not contain active response functionalities on suspected threats through utilizing basic surveillance methods alone. The proposed project is unique in that it is focused towards increasing security in terms of utilizing multiple detection levels and authentication layers to bring better accuracy and dependability.

In the middle, it is installed with Raspberry Pi 4 as a processing unit, which performs data processing, authentication, and immediate alerts. A camera module and a PIR sensor serve as the primary trigger devices, initiating security measures whenever they sense movement. The system is designed to detect authorized and unauthorized movement, thus allowing for immediate and automatic action. Along with it, there exists a single web-based interface with controlled users enabling remote management and monitoring of the system for easy, secure management tool.

Figure 1: Login page of website

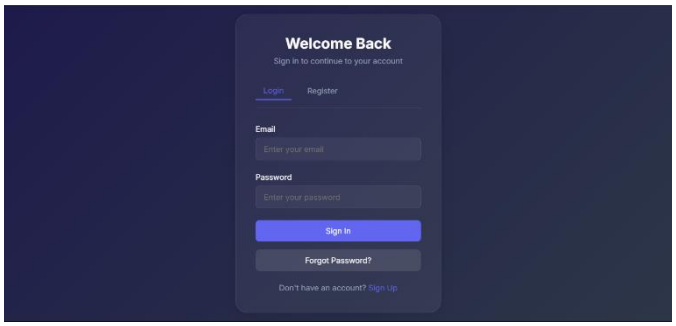


Figure 2: Dashboard after login on website

After login in website first dashboard appears where it shows environment details. It also gives an option to add users, these users don't have any time limit, Then, in add guests the user with time limit can be added after that time expire the guest will be unknown again. Frames of unknown faces and violence detection are available in folders option where these frames are organized by date and time. Also, there is option to watch live and door status either closed or opened. Also through authentication user can reset system, see the entry time and date of authorized users.

The system has been added with advantage of flexibility in scenarios where real-time security and automation are essential. While traditional solutions only provide generic video surveillance, the project involves an intelligent decision-making framework, where security threats are detected in real-time and tackled systematically. Multi-layered authentication adds an additional layer of security, minimizing risks of unauthorized entry.

4. METHODOLOGY

The system proposed has a number of layers of protection to authenticate and identify people in an environment. The controller is a processing unit that manages different sensors and decision algorithms to produce an adaptive response to threat.

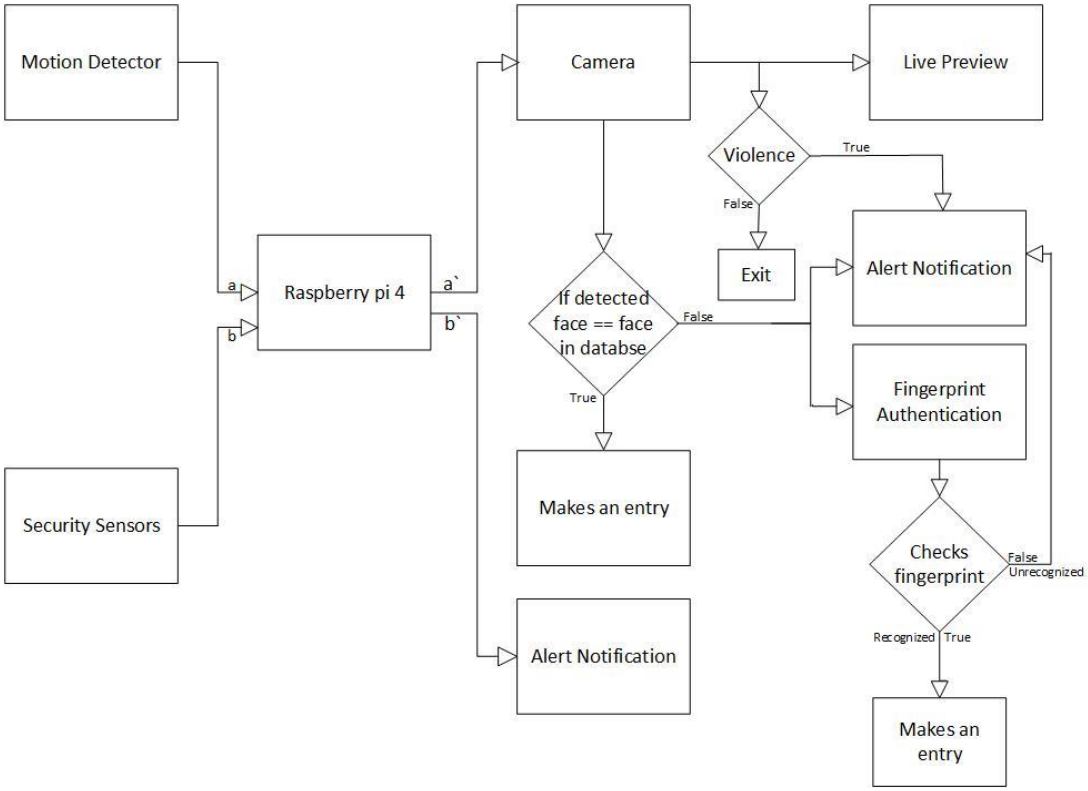
i. Motion Detection & Initial Triggering

The system will only begin to function when motion is present in the monitored area. During startup, the motion sensor triggers alerts into the processing unit, which activates extra surveillance work. Safety sensors have the task of another level of monitoring to watch for unwanted entry.

ii. Visual Input & Identification

A live video input module takes live video and passes it to a live preview interface. Simultaneously, identification is done by matching the person with a stored database. If identified, he/she gets a secure entry record and nothing else is saved. If unknown, other verification processes are called.

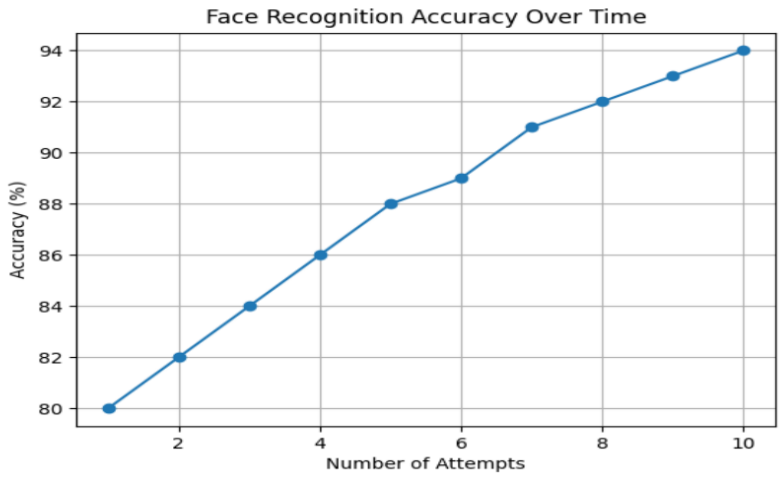
Figure 3: Workflow of System



iii. Threat Analysis & Security Response

The system employs an analysis process to verify whether the identified individual is performing suspicious activity. In case of a potential threat, it alerts in real time.

Chart 1: Graph of Face Recognition Accuracy



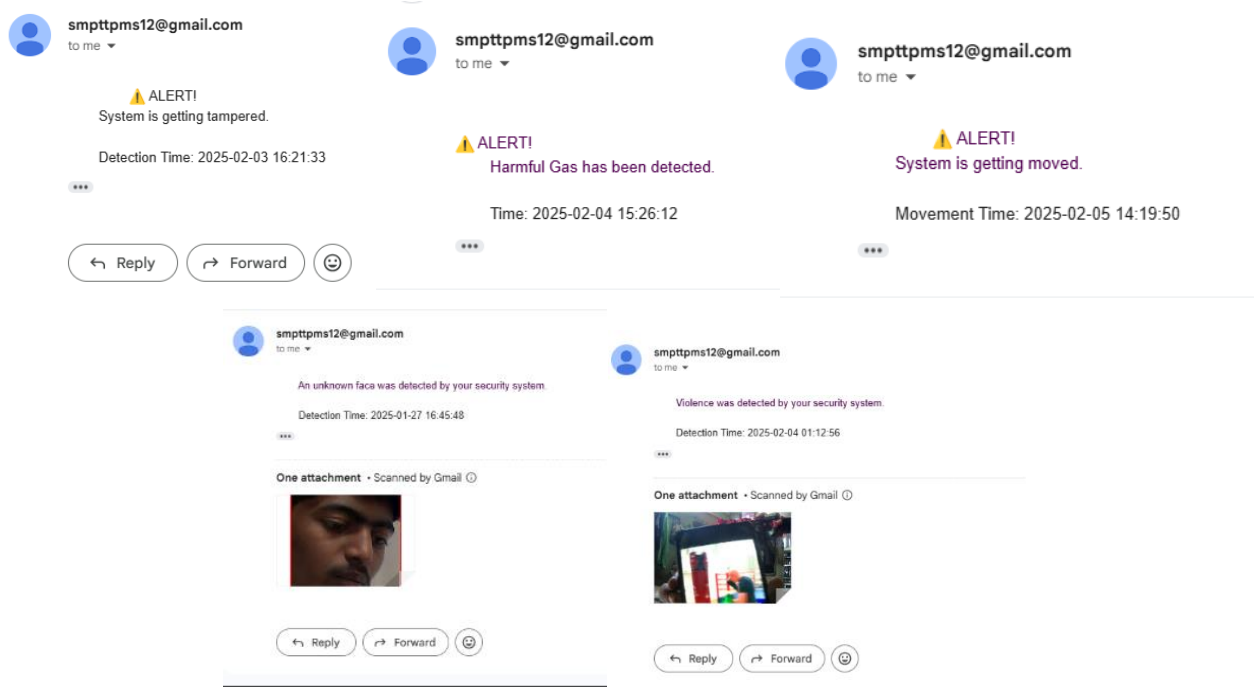
iv. Biometric Verification & Secure Access

Secondary biometric verification is performed if needed. The system checks against authentic stored data through a match-check. Authorized users are permitted, and unauthorized accesses receive an alert.

5. RESULT

The Shield Sight Advanced Frith System was implemented successfully, which demonstrated its capability for real-time threat detection, authentication, and immediate security response. The system was efficient in motion detection with PIR sensors, which triggered the camera module to identify the face of a person, and this was 92% efficient in recognizing authorized and unauthorized persons. The system tracked attempted illegal access with timestamps, and instant messaging was delivered through Gmail for informing the users about possible security breaches. The biometric authentication mechanism served as an second-layer of security.

Figure 4: Screenshot of G-Mail Alert



Remote monitoring was achievable via the web-based interface of the system, and the users could monitor live camera feeds, access logs, and manage user authentication. Guest user management was a robust technique of time-based access restriction, remote revocation of rights on the passage of the elapsed time. Security operations and processing of data were high-speed in Raspberry Pi 4, having the best performance of the system without undue latency and faster response. The system reduced the human touch to a large extent without compromising reliability and security and thus made it an economical and scalable solution for home, office, and high-security applications.

6. CONCLUSION

The Shield Sight Advanced Frith System presents a comprehensive overhaul from traditional security systems in that it employs smart automation and multi-level authentication. The complementarity between the motion detection, facial recognition, biometric identification, and real-time notification provides an active security response with less human participation and increased safety and reliability than traditional surveillance systems. The inclusion of a straightforward web-based interface offers remote monitoring and efficient control of users and visitors. The project not only enhances security but also provides

flexibility for different applications, ranging from home security to high-security business settings. With the inclusion of automation and real-time decision-making, the system redefines contemporary security solutions.

7. ACKNOWLEDGEMENT

The authors are truly grateful to the useful suggestions and advice of Dr. S. B. Dhoot, Head, Department of Electronics & Telecommunication, Government Polytechnic College, Chhatrapati Sambhaji Nagar. His guidance and experience have played a crucial role in shaping the research content and direction of this review paper. His encouragement and valuable criticisms have played a crucial role in refining the work and removing problems faced while preparing it. The authors would also like to thank Dr. Dhoot for his constant encouragement, which has been the major factor in the success of this paper.

8. Authors' Biography

i. Ankur Chopde – Polytechnic Student, Electronics and Telecommunication, Government Polytechnic of Chh. Sambhajinagar.
ii. Radhika Muley – Polytechnic Student, Electronics and Telecommunication, Government Polytechnic of Chh. Sambhajinagar.
iii. Dr. S. B. Dhoot – Head of Department, Electronics and Telecommunication, Government Polytechnic of Chh. Sambhajinagar.

References

1. Raju A Nadaf, S.M. Hatture, Vasudha M Bonal, Susen P Naik, “Home Security against Human Intrusion using Raspberry Pi,” ScienceDirect Volume 167, 2020, Pages 1811-1820, doi.org/10.1016/j.procs.2020.03.200.
2. Arti Kate, Sayali Somwanshi, Vaibhav Magar, Vaibhav Vyavahare, “IOT Based Visitor Monitoring System Using Raspberry PI,” IJSRSET Volume 6, Issue 2, DOI : 10.32628/IJSRSET196299
3. Mohanad Abdulhamid, Singoee Sheshai, “DESIGN OF SECURITY SYSTEM BASED ON RASPBERRY-PI,” Sciendo DOI: 10.1515/SBEEF-2019-0022
4. Dr. Nagalakshmi Venugopal, Chalamalasetty Edward Pradeep Kumar, Goutham Prashanth V G, Manoharan E, Kesavamurthy K, “IoT based Security System using Raspberry Pi,” IJERT, Vol. 9 Issue 02, February-2020 IJERTV9IS020355.
5. Shital A. Patil, Deepak B.Kadam, “ Security System using Raspberry Pi,” IJITEE Volume-8 Issue-11, September 2019, DOI: 10.35940/ijitee.J1163.0981119
6. Dhanshri Mali, R. T. Patil, Nagaraj Dharwadkar, Chaitanya R. Devale, Omprakash Tembhurne, “Real-Time Smart Surveillance System Using Raspberry Pi,” ssrn.com/abstract=3357807
7. Mekecha Banchigize Bazezew, “Home Surveillance and Alert System using Raspberry Pi Zero W and GSM Modem with MQTT Protocol,” IJAINN , Volume-3 Issue-2, February 2023, DOI:10.54105/ijainn.D4071.023223
8. Md. Rakib Ahsan, Mohammad Shamsul Arefin, . Sheikh Zarif Ahmad, . Md.Aminul Bari, “Implementation of IOT based Smart Security and Home Automation System,” IJERT Vol. 8 Issue 06, June-2019, IJERTV8IS060732.
9. Abdu Subhan, Abhilash Nair, Alen Johny, Ms. Tinu Thomas, “Advanced Home Automation and Security Systems Using IoT,” IJERT Volume 11, Issue 01

10. Bharti Chouhan, Tasneem Banu , Pankaj Rathi, “Advanced Home Security System,” IJERT IJERTCONV2IS10048.
11. Keerthana Chandran, “A Review Of Iot-based Surveillance,” IJERT Volume 11, Issue 01.
12. Vikrant H. Modi, Ami A. Patel, “Intrusion Detection System: A Review,” IJERT Vol. 2 Issue 11, November – 2013, IJERTV2IS110067
13. Mihir Upagade, Jaideep Dongare, Anshul Ajapuje, Uttakarsh Panse, Rohan Kamble, “Iot Based Home Security System,” IJERT Vol. 12 Issue 03, March-2023, IJERTV12IS030015
14. Prof. Muzaffar Khan, Nusrat Khan, Pooja Yadav, “A Review On Iot Based Smart Security System Using Raspberry Pi,” JETIR , Volume 6, Issue 5 JETIRBV06080.
15. Srushti A. Nagtode, Prof. Mrs Y. A. Sadawarte , Prof. Mrs D. M. Khatri, Prof. Prashant R. Indurkar, “Review paper of IoT Based Smart Home Security System,” IJAEM Volume 3, Issue 6 June 2021, DOI: 10.35629/5252-0306581585.
16. Ankur Chopde, Radhika Muley, Sakshi Vishwakarma, Nandini Potdar, “An IoT Based Multipurpose Frith System: A Review,” IRJET Volume 12, Issue 3, February 2025.