

¹Shivangi Agarwal,
²Yogita Mistry,
³Savita Bhosale,
⁴Atharva Sagare
⁵Nilam Patil

Development of IOT-based Smart Anti – Theft Latch



Abstract: - In our day to day lives, security is of utmost concern. Everyone wants to be as secured as possible. This paper develops an Internet of Things (IoT)-based smart security system and supports the concept of a "IOT close to life and easy to use". One of the many useful applications of IoT is home security; among other things, we're leveraging it to build affordable home security systems. The IoT is a network of physically connected objects that can exchange data and communicate with one another without the need for human intervention. The simplicity of setup, low cost, and minimal maintenance are some of this system's key benefits. This system is executed with the help of Raspberry Pi 3B. Face recognition system used determines if the individual is lively enough to receive authorization. If an unauthorized access is detected then the buzzer will be triggered and an alert notification will be sent on an app which is designed for the owner which will also include a photo detected by the camera and with an option to reset the buzzer. This system comprises of dual authentication that is Radio Frequency Identification (RFID) key and a face recognition system. This approach is able to protect the homes from intrusions by continuous detection of the suspicious actions using soft computing, that is, Convolutional Neural Network (CNN) algorithm for face recognition.

Keywords: *Raspberry Pi 3B, Face recognition, Inexpensive, Low maintenance, soft computing, Security System, Internet of Things, Camera, Radio Frequency Identification, Convolutional Neural Network.*

I. INTRODUCTION

The rate of theft and robberies has risen sharply in recent years. Home safety is of utmost importance to the owners. So, an overview of Smart Anti – Theft latch has been presented which comprises of two-way authentication using RFID system and Face Recognition system. With the advancement in crime rates, there is an alarming significance for the need of security of the houses. Basically, the goal is to provide a security system for the houses which is more reliable and cost efficient. This will help the owners to keep track on their houses throughout the day. IoT gives users greater access to and control over environments and devices that are not currently connected to the internet.

The rate of larceny has risen sharply in recent years. It was found in the study which was done in 2009 that, even though the people who don't have their own security system the risk of the robberies have been decreased in that area due to the increase in the number of home security systems present in that area. This hampers the reputation of the school as well. Thus, there is an alarming need of a secure and reliable system which assures the security of the houses to their owners. In addition to providing protection, a security system helps prevent crime and makes the neighborhood a safer place for everyone. Therefore, we have presented this design to achieve protection from theft and burglary instances that are on a rise since past few decades.

This paper proposes a system that uses the RFID technology and a face recognition technology which makes the system staunch. The proposed system will also have the buzzer which will be triggered if an intruder tries to break into the house and will help to avoid the burglary. The owner will be notified about the theft or any suspicious activity in front of his house through an app which will be designed for the owner. The key contributions of the proposed research work in this paper are as follows: -

- To design and develop an automated RFID and face recognition-based system.
- To provide protection to the homes to ensure the safety of the valuables.
- To design a low-cost system which will be affordable to any common person who can use it for their houses.
- An intuitive user interface is provided by this system. This solution is also usable by anyone with limited Android understanding.

¹*Corresponding author: shivangi.agarwal@rait.ac.in

^{1,2,3,4,5}Ramrao Adik Institute of Technology, D.Y. Patil Deemed to be University, Nerul, Navi Mumbai-400706, India

²yogita.mistry@rait.ac.in, ³savita.bhosale@rait.ac.in, ⁴atharvasagare27@gmail.com, ⁵nilam.patil@rait.ac.in

Copyright © JES 2024 on-line : journal.esrgroups.org

The rest part of this paper is arranged as follows: Literature survey and related work with respect to existing systems is given in Section II. Section III deals with proposed methodology, which consists of architecture of the system, hardware and software components, and proposed algorithm. The results and analysis have been briefly explained in Section IV. The conclusion and future work of the paper are discussed in Section V.

A. Literature Survey

The objective of this study is to make a cost effective and interesting security alarm for highly authentication places. The setback of this study is that there is no system to disarm the alarm also the exact position of an intruder cannot be determined. V.Krishnaveni et al. [1]. The aim of this study is to identify the unapproved passage and criminal operations by making use of particular sensors. The stumbling block of this study is that to make aware the neighbours and the security about the intrusion the buzzer is required to meet the demand of the work. Vijetha T S, Meghana et al. [2]. Using the proper information security mechanisms, this study aims to provide secure, controllable, and even personalized real-time online monitoring, as well as features like alarm linkage, plan management, remote control, security, remote maintenance, online upgrade, management, and decision support. In this study security will become an issue as more people use smart home devices due to which the range of security concerns may arise. Chanthaphone Sisavath et al. [3]. The work on this study reflects the implementation of the Near Field Communication (NFC) door lock which is a digital door lock for home automation also it is user friendly and installation is easy. The restrictions of this study is that NFC devices can only work in shorter distances also the power consumption is more in the NFC enabled devices. Jose Pacheco et al. [4]. This paper presents a system which is designed to track an electric bike by using Zigbee technology which is used as the wireless communication module that is energy efficient and allows multiple devices to communicate also will help the electric bike user to access the location of the electric bike on his/her smart device. Zigbee based systems are short range and they are not as secure as WIFI based secured system. Veerandi Kulasekara et al. [5]. The intent of this study describes the technology used for security systems that uses CCTV for security purpose which detects the actions of the person and is secured by motion sensors and sound detection sensors. The drawback of this study is that it is vulnerable and the price of home automation installation is very high. Manjunath M et al. [6]. The work in this study describes that a Smart Home Security System (SHSS) is designed by using "Wechat" platform which is China's do everything app and use Zigbee network to achieve the functions like collecting and detecting data, transmitting and processing information for better service design. The setback of this study is that Wechat has no end-to-end encryption security feature also IoT technology which will control system software development is neither used and Zigbee is risky to be used for private information. Yaling Hong et al. [7]. The aim of this study is that to make the use of millimetre wave (mmwave) radar which will introduce a biometric system for non-contact speaker verification for IoT smart home appliances. The misfortune in this study is that millimeter wave (mmwave) radar does not provide the accurate distance measurements of nearby objects which might weaken threat identification process. Yudi Dong et al. [8]. The study focuses about various aspects of deep learning and Convolutional Neural Network (CNN) specifically, and carries out image detection and recognition 1. and also uses Modified National Institute of Standards and Technology (MNIST) dataset and Canadian Institute for Advanced Research (CIFAR-10) dataset. The downside of this study is that the accuracy of image recognition is quite less. Rahul Chauhan et al. [9].

2. An empirical assessment of the face recognition system is presented in this research using Convolutional Neural Network (CNN) architecture. The prominent features of the proposed algorithm are that for the outputs of the first and final convolutional layers it employs the batch normalization and that makes the network reach higher accuracy rates. The major barrier in this study is that batch normalization requires sufficiently large batch sizes to generate good results. This prohibits from exploring higher capacity models that would be limited by memory. Musab Coskun, Aysegul Ucar et al. [10]. Some recent works are [11,12,13,14,15]. Table 1 enumerates the works that are currently available.

TABLE 1: Summary of Related Work

| Author | Description | Limitations |
|--------------------------|---|---|
| V.Krishnaveni et al. [1] | To make a cost effective and interesting security alarm for highly authentication places. | There is no system to disarm the alarm also the exact position of an intruder cannot be determined. |

| | | |
|----------------------------------|---|--|
| Vijetha T S, Meghana et al. [2] | To identify the unapproved passage and criminal operations by making use of particular sensors. | To make aware the neighbours and the security about the intrusion the buzzer is required to meet the demand of the work. |
| Chanthaphone Sisavath et al. [3] | Making use of appropriate information security mechanisms to provide secure, controllable and even personalized monitoring, and service functions such as decision support. | Security is an issue as more people use smart home devices due to which the range of security concerns may arise. |
| Jose Pacheco et al. [4] | Implementation of the Near Field Communication (NFC) door lock which is a digital door lock for home automation also it is user friendly and installation is easy. | NFC devices can only work in shorter distances also the power consumption is more in the NFC enabled devices. |
| Veerandi Kulasekara et al. [5] | Aims to track an electric bike by using Zigbee technology. | Zigbee based systems are not as secure as WIFI based secured system. |
| Manjunath M et al. [6] | Uses CCTV for security purpose which detects the actions of the person and is secured by motion sensors and sound detection sensors. | It is vulnerable and the price of home automation installation is very high. |
| Yaling Hong et al. [7] | Describes that a Smart Home Security System is designed by using "Wechat" platform which is China's do everything app and use Zigbee network. | Wechat has no end-to-end encryption security feature also IoT technology which will control system software development is neither used. |
| Yudi Dong et al. [8] | To make the use of mmwave radar which will introduce a biometric system for non-contact speaker verification for IoT smart home appliances. | Mmwave radar does not provide the accurate distance measurements of nearby objects. |
| Rahul Chauhan et al. [9] | Uses deep learning and Convolutional Neural Network (CNN) in particular and performs image recognition and detection. | The accuracy of image recognition is quite less. |
| Musab Coskun et al. [10] | It employs the batch normalization for the outputs of the first and final to reach higher accuracy rates. | Batch normalization requires sufficiently large batch sizes to generate good results. |

B. Proposed Methodology

The proposed solution is an add-on to the existing available systems for safety of houses using cost effective technologies like RFID, Face Recognition and IoT. The proposed solution in this paper has many additional features and safety measures.

II. ILLUSTRATIONS

A. System Design: -

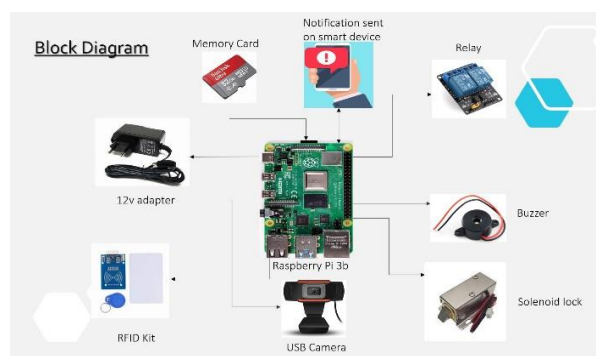


Fig. 1 Block Diagram

1. Raspberry Pi:

The Raspberry Pi foundation in the UK invented a small sized i.e., card sized minicomputer called Raspberry pi. Raspberry pi is the system’s main controller, taking input from all the sensors and delivering suitable actions as an output. It has the capability of doing everything which you expect a desktop computer to do.

2. Buzzer:

The buzzer is an audio signaling device that converts the audio to sound. It is given a power supply through dc voltage and is commonly used in timers, alarm devices, computers, etc.

3. Double Channel 5v Relay:

The 2-Channel 5V Relay Module is a relay interface board that may be controlled directly by a variety of microcontrollers, including Arduino, AVR, PIC, and ARM. The relay is controlled by a low-level triggered control signal (3.3-5VDC). The input voltage range for 5V relay signals is 0-5V.

4. Radio Frequency Identification Kit:

RFID uses radiofrequency waves for contactless data transmission. Radio waves are used to read and capture the stored information on a tag which is attached to an object, giving a specific identifier for an object. Many of the organizations are beneficial by using the RFID technology and the applications of RFID has huge demands in wide range of industrial sectors.

5. USB Camera:

USB camera is an electronic device that can be attached a computer system through various USB plugs in sources available on the system.

6. Solenoid Lock:

The 5V Solenoid Lock has a slanted cut slug and a sturdy mounting bracket. It's essentially an electronic lock for a standard cabinet, safe, or door.

7. Class 10 SD Card:

Class 10 Secured Digital (SD) card indicates that the card has a minimum non-fragmented sequential write speed of 10 MB/s and operates in the High-Speed bus mode.

8. 12V Adapter:

A 12V DC output is generated from the 120V AC or 240V AC input using a combination of transformers, diodes and transistors. 12V regulated power supplies and 12V unregulated power supplies are the two categories of 12V power supplies.

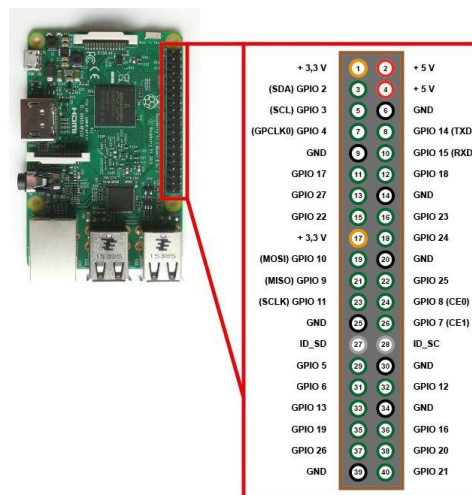


Fig. 2 Pin configuration of Raspberry Pi

B. Software technologies used -

1. Python:

Python is a dynamically semantic, interpreted, object-oriented high-level programming language. Its high-level built-in data structures, along with dynamic typing and dynamic binding. Its straightforward, easy-to-understand syntax promotes readability, lowering program maintenance costs. Modules and packages are supported, allowing for program modularity and code reuse. Python libraries are available in source or binary form for all major platforms and are free to download.

Programmers prefers python because of its productivity and enhancement which it delivers. Because there is no compilation phase, the edit-test-debug cycle is exceedingly fast.

2. **MySQL:**

MySQL is the most extensively used open-source database in the world (back-end). It is the most PHP-friendly database, as PHP-MySQL is the most popular open-source scripting database perfect choice. The MySQL user interface provided by WAMP, LAMP, and XAMPP servers is the most user-friendly and significantly decreases our workload.

3. **HTML:**

HTML (Hyper Text Markup Language) is the coding that organizes a web page's structure and content. The HTML documents are accepted by the Web browser from a locally stored file or a web server and then converted into multimedia web pages. At first HTML suggests to show the documents and then the web page structure is described logically. Components that make HTML pages are called as HTML elements. The construction of organized documents is done by indicating the diagrammatic structure considering text elements like headers, paragraphs, sections and other elements.

4. **JavaScript:**

Web pages are created using the scripting language known as JavaScript. It enables us to add dynamic behavior to the homepage as well as unique effects. It is mostly used on websites for validation purposes. JavaScript permits us to do complicated tasks as well as allows websites to communicate with users. Much of the structured programming syntax from C is supported by JavaScript. It distinguishes between statements and expressions.

5. **CSS:**

Cascading Style Sheets is a stylesheet computing dialect for describing the appearance of an HTML or XML document. Along with HTML and JavaScript, CSS is a key component of the World Wide Web. Its layout, colors, and typefaces are all meant to allow for the partition of display and content. If the article is viewed on a smartphone, it may have additional formatting requirements.

6. **Raspbian Operating System:**

Raspbian is a uncertified port of Debian Wheezy armhf that has had its compilation settings tweaked to produce optimal" hard float" code for the Raspberry Pi. For applications that rely heavily on floating point arithmetic operations, this results in much faster performance. The use of advanced instructions on the Raspberry Pi's ARMv6 CPU will improve the performance of all other programmes.

C. Algorithm:

1. Start, register the details.
2. Enter the authentication details.
3. If valid, show the RFID card/key for verification. If not, go to step 2.
4. If RFID matched, show face to camera for recognition. If RFID not matched, stop.
5. If face matched, latch opened. If not, buzzer is triggered.
6. Stop.

D. Flow Chart:

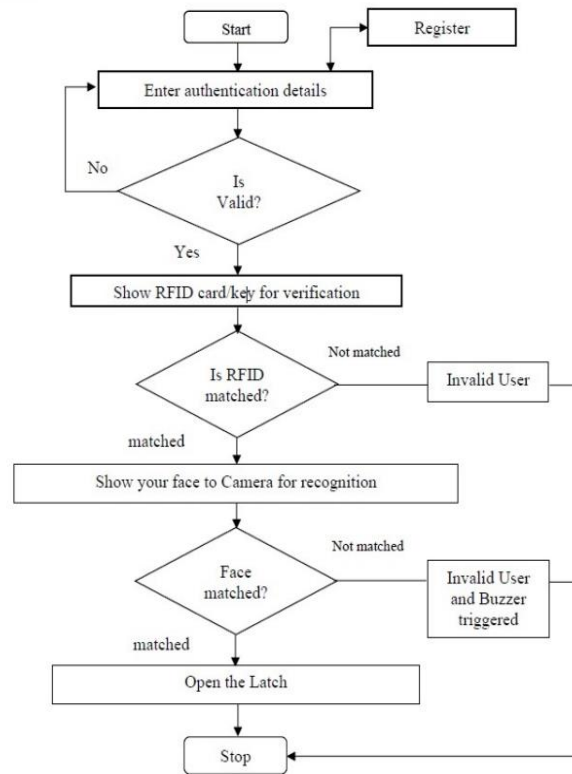


Fig. 3 Flow Chart of the system

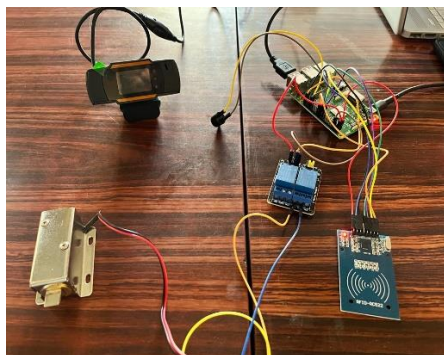


Fig. 4 Hardware implementation of all components

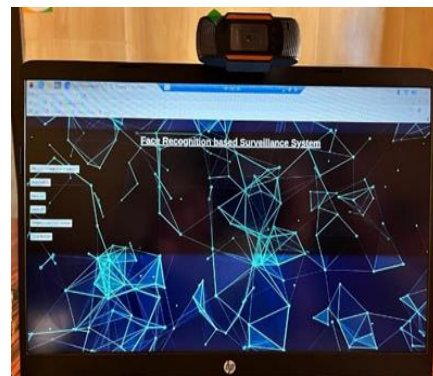


Fig. 5 Web Application Interface

III. USE CASE DIAGRAMS:

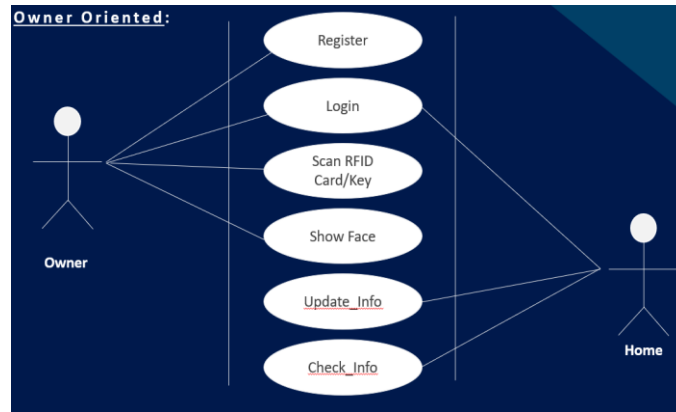


Fig. 6 Owner Oriented Case Diagram

The above figure 6 is the use case diagram which tells us about the various actions that are going to be performed by the Smart Anti-Theft Latch respectively. The various actors are owner and the home anti-theft latch. The owner is identified after the RFID information is scanned and the face is matched with the database. Thus, the owner is granted access into his after the dual authentication.

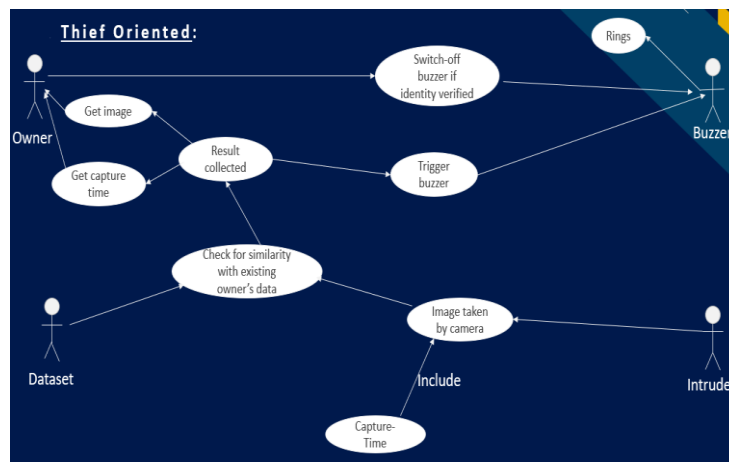


Fig. 7 Thief Oriented Case Diagram

The above figure 7 is a use case diagram which is thief oriented for the smart anti-theft latch. The various actors are owner, data-set, intruder and buzzer. If an intruder tries to break in an image will be taken by camera including capture time, and it will be checked for similarity with the existing owner's data by the data-set. If result collected is mismatched, the image will be sent to the owner and the buzzer will be triggered. If the mismatched identity is verified by the owner, then the owner will reset the buzzer.

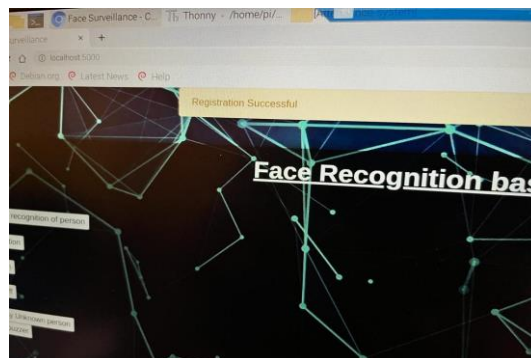


Fig. 8 Message shown after successful registration

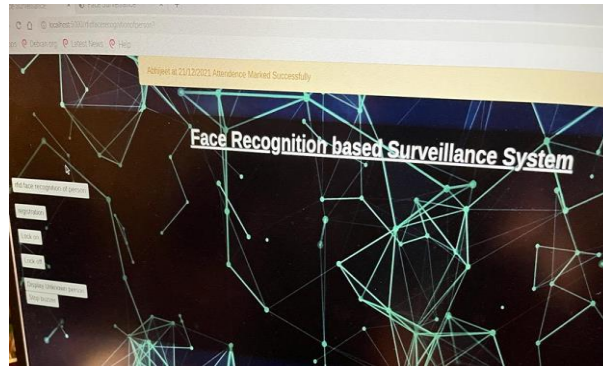


Fig. 9 Message indicating successful latch unlock

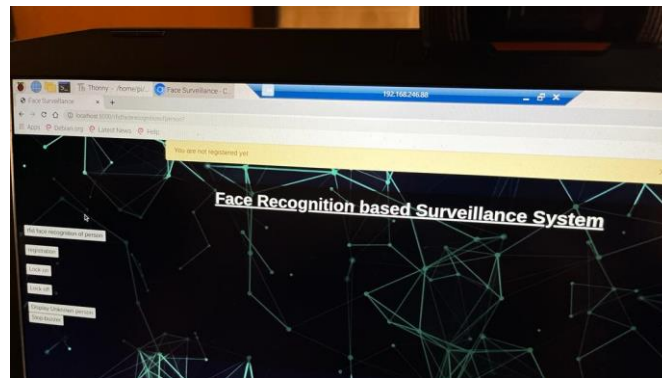


Fig. 10 Message for unregistered data

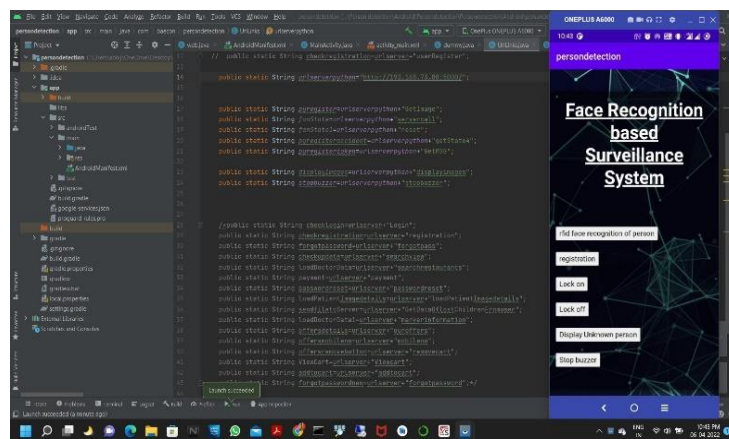


Fig. 11 Android Application

The above Figure 11 gives the brief idea about the Android Application which is designed for the owner to control the system. This app basically casts the web application interface which will help the owner to control the system and keep a track from his or her smart device.



Fig. 12 Screenshot of the app interface in the phone

The above Figure 12 shows the interface of the Android Application which is installed in the owner's smart phone.

IV. RESULT AND DISCUSSION

The study resolves one of the major home security issues. It keeps a track and helps to avoid the intrusion. The experimental setup consists of hardware and software. The hardware components comprise of Raspberry Pi Model 3B, USB camera, RFID tags and readers, Double Channel 5v relay, Solenoid Lock, 12V Adapter, 32 GB Class 10 memory card, Buzzer. In this proposed system, the software comprises of web application is used by the owner, the android application used by the owner and a dataset where the entire data is stored. The system was deployed using Windows 10 operating system with Intel 8th gen i5 processor, 8GB RAM and 1TB hard disk.

This study related papers also discusses there is no system provided to disarm or reset the buzzer and also the exact position of an intruder cannot be determined. Existing systems have also used the NFC devices that can only work in shorter distances and have more power consumption. Another research paper presents a system that uses ZigBee technology. The drawback of this kind of system is that it is short range and is not as secured as WIFI based systems. One of the studies describes that Smart Home Security System is designed by using Wechat platform. However, the setback of this study is that it has no end-to-end encryption security feature.

V. CONCLUSION AND FUTURE WORK

In the proposed system Raspberry Pi is been used which is very much handy, highly effective, also inexpensive and portable as well. Due to security reasons the home security alarm systems are highly in demand. In this study, the designed security system will have the capability of detecting the intrusion. If something goes wrong, the system will identify any illicit activity while the user is not there and alert them.[2] In order to address security issues and lessen or eliminate theft, the system is built as an anti-theft device. Small-scale personal area surveillance is appropriate for this system. such as the parking entry, bank locker room, and private office cabin. The benefit of this study is that the implementation is easy and low priced with superior quality. It is a flexible system. People who want to protect their properties and want to restrict access can use such type of beneficial system. This method is really affordable and simple to use, so anyone can make use of this system.

REFERENCES

- [1] V.Krishnaveni, A.Priyanga, V.Vidya, G. GaneshKumar , "An Advanced IOT based Antitheft Security System with Video Monitoring Facility", SSRG International Journal of Computer Science and Engineering, March, pp. 50-54, 2019.
- [2] Vijetha T S, Meghana, Namratha S H, Nayanashree K S and Kavyashree G B, "Antitheft Sensor Controlled Home Security System", International Journal of Electronics and Communication Engineering and Technology (IJECET), Volume 11, pp. 1-6, May-August 2020.

- [3] Chanthaphone Sisavath, Lasheng Yu, "Design and implementation of security system for smart home based on IOT technology" *Procedia Computer Science*, 10th International Conference of Information and Communication Technology (ICICT-2020), Volume 183, pp. 4-13, 2021.
- [4] Jose Pacheco, Karen Miranda, "Design of a low-cost NFC Door Lock for a Smart Home System", 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 9-12 September 2020, 1, pp. 1-5.
- [5] Veerandi Kulasekara, Pasan Dharmasiri, Pham Chi Thanh, Ilya Kavalchuk, "Novel ZigBee-Based Smart Anti-Theft System for Electric Bikes for Vietnam", 2020 RIVF International Conference on Computing and Communication Technologies (RIVF), 14-15 October 2020 , pp. 1-6.
- [6] Manjunath M, Venkatesha G, Dinesh S, "Raspberry Pi Based Anti-Theft Security System using Home Automation for Multi-Level Authentication", *Embedded-Systems and Signal-Processing (PiCES) – An International Journal* Volume 4, pp. 249-253, January 2021.
- [7] Yaling Hong, Haonan Long , "Research and Development of Smart Home Security System Based on Wechat Control", *Journal of Physics: Conference Series*, Volume 1915, Computer Engineering, pp. 1-6, July 2021.
- [8] Yudi Dong, Yu-Dong Yao, "Secure mmWave-Radar-Based Speaker Verification for IoT Smart Home", *IEEE Internet of Things Journal*, Volume 8, pp. 1-12, September 2020.
- [9] Rahul Chauhan, Kamal Kumar Ghanshala, R.C Joshi, "Convolutional Neural Network (CNN) for Image Detection and Recognition", 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), pp. 278-282, 15-17 December 2018.
- [10] Musab Coskun, Aysegul Ucar, Ozal Yildirim, Yakup Demir, "Face Recognition Based on Convolutional Neural Network", 2017 International Conference on Modern Electrical and Energy Systems (MEES), pp. 376-379 15-17 November 2017.
- [11] Farahsari, Pooyan Shams, Amirhossein Farahzadi, Javad Rezazadeh, and Alireza Bagheri. "A survey on indoor positioning systems for IoT-based applications." *IEEE Internet of Things Journal* 9, no. 10 (2022): 7680-7699.
- [12] 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, 1 May1, 2022, doi: 10.1109/JSEN.2022.3161797.
- [13] M. S. Abdalzaher, M. M. Fouda, H. A. Elsayed and M. M. Salim, "Toward Secured IoT-Based Smart Systems Using Machine Learning," in *IEEE Access*, vol. 11, pp. 20827-20841, 2023, doi: 10.1109/ACCESS.2023.3250235.
- [14] L. J. Baptist Andrews, S. D and R. A. Raj, "IOT Based Surveillance Camera with GPS Module," 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2023, pp. 1-3, doi: 10.1109/SCEECS57921.2023.10062961.
- [15] Rock, L.Y., Tajudeen, F.P. & Chung, Y.W. Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective. *Univ Access Inf Soc* 23, 345–364 (2024). <https://doi.org/10.1007/s10209-022-00937-0>