Enhancing Home Security with Pressure Mat Sensors: A Multi-modal IoT Approach

Karel Veerabudren(✉), Visham Ramsurrun, Mrinal Sharma, and Amar Seeam

Middlesex University, Uniciti, Flic-en-Flac, Mauritius
{k.veerabudren,v.ramsurrun,m.sharma,a.seeam}@mdx.ac.mu

Abstract. Home security is a major concern worldwide, and there are various solutions available, but with limitations. This paper proposes a novel security system that overcomes the limitations of current systems by using piezoresistive sensors placed inside a mat to detect intruders with varying levels of pressure intensities. The proposed system incorporates a camera and a CNN algorithm with the EfficientNet model to detect whether the object is a human, and it is equipped with features like an email and SMS notification mechanism, backup battery, and a sophisticated tracking mechanism. The proposed system is highly resilient to tampering or circumvention and outperforms existing security systems in terms of being non-intrusive, providing tracking features for the intruder, and being resistant to blackouts. This paper documents the research, development, testing, evaluation process, and contributions made to address the security challenges by developing an affordable, easy-to-use, and effective home security system.

Keywords: IoT Home Security · Floor sensors · Intruder detection

1 Introduction

Smart home security refers to the use of IoT devices, which consist of a network of interconnected devices with technologies put in place [1] to enhance the security of a domicile. This includes using cameras, sensors, and notification alarms, with the key benefit of being remotely controllable and accessible [2]. These systems have been growing in popularity, and one reason is the increasing risks of home intrusions [3]. In 2020, burglary ranked the most frequent crime in the United States and is among the most common crimes committed globally. SafeHome [4] conducted a study that revealed nearly half of the American population has been a victim of burglary, with 47.64% of them being present during the crime. The high crime rates and risky nature not only result in financial loss but also inflict emotional trauma on victims, affecting communities and society. The widespread use of traditional security mechanisms combined with IoT systems in households highlights the clear necessity for home security. However, these systems are not always effective, as burglars can bypass them and go undetected. Additionally, some systems have a high rate of false positives. In her research the author Gonzalez [5], expounded on the issue of security system sensitivity, highlighting its

A. Seeam et al. (Eds.): InterSol 2023, LNICST 541, pp. 81–95, 2024.
https://doi.org/10.1007/978-3-031-51849-2_6

potential obsolescence. They also presented a staggering statistic, with false positives accounting for up to 95% of triggered alerts. The susceptibility of sensors to various environmental and lighting factors has contributed to this phenomenon, resulting in the wastage of valuable resources such as time and money.

In addition, the reliance on internet connectivity for all IoT security devices also presents a significant security concern [6]. As noted by Tholen [7], in the event of a power outage, the entire system becomes vulnerable and unable to monitor the home. This outage can make the system an ideal target for burglars, who can exploit the security gap to gain undetected access to the property. Even more concerning is that homeowners who are away during the blackout may not be aware of the outage until it is too late, leaving them vulnerable to thefts and property damage. Therefore, it is crucial for homeowners to have contingency plans in place in case of power outages to ensure the continued security of their homes.

This paper presents the results of developing a non-intrusive multi-modal home security system using a mat-based flooring detection system. The system detects intruders by ensuring they step on the floor, and a heatmap displays their live location. False positives have been reduced using machine learning algorithms to confirm the presence of humans. The system is also blackout-resistant, and the homeowner is notified through different channels. A web application displays the heatmap and provides camera access, with a database to store intrusion and blackout history. Overall evaluation is based on the success of the system's effectiveness, blackout resistance, and user-friendliness.

The paper is organized as follows: Sect. 2 reviews existing home security systems and their sensors. Section 3 describes the proposed design and the development of its hardware and software to achieve the paper's aims and objectives. The testing of the system is detailed in Sect. 4, followed by an evaluation in Sect. 5. Finally, Sect. 6 concludes the paper with potential future pathway considerations.

2 Literature Review

2.1 Background

Technological advancements on the Internet of Things (IoT) have expanded the capabilities of home security systems. These systems now integrate with traditional security measures to provide enhanced protection against intruders. A modern home security system comprises input devices, a processing unit, and output devices. The input devices include sensors that monitor the home environment, and the data collected is transmitted to the processing unit, which is typically a microcontroller. The microcontroller analyses the data received and sends a signal to the output device, usually an alarm if any abnormalities are detected.

This concept has proven to give homeowners greater security and peace of mind. Various input sensors can further improve the accuracy and precision of the security system, providing even greater reassurance to homeowners—for example, the ability to detect fire/smoke and alert the homeowner via an application. Additionally, the system can detect intrusion using motion, door sensors, and a security camera. When the sensors detect unusual activity, such as motion or a door opening, a signal is sent to the microcontroller. The microcontroller receives the data from the sensors, analyses the

data based on predetermined thresholds, and decides whether to notify the homeowner. If necessary, the microcontroller sends a notification to the respective parties via a Wi-Fi module, which enables it to connect to the home router. If an alarm is present, it will automatically trigger when the notification is sent.

For instance, Desnanjaya and Arsana [8] discuss creating a home security monitoring system using Raspberry Pi as the control centre. The system includes various sensors such as PIR, raspicam, temperature and gas. Telegram is used to send notifications from the Raspberry Pi to users. The system can detect intruders, take pictures, monitor temperature, and detect gas or smoke. Sharma et al. [9] discuss an affordable and innovative smart home monitoring system called RaspiMonitor. The system aims to provide a comprehensive smart home architecture that ensures the safety and security of its environment using PIR and gas sensors while also reducing energy wastage. Users can then control their homes and monitor their usage through the web application. In addition, there is also the Ring Alarm Pro [10], which is a commercial product. The system features an integrated router that allows the different sensors, such as motion and door sensors, to be easily connected. Other devices, such as smart bulbs or door cameras, can be paired easily. The whole system can be controlled through its mobile application.

The following section reviews some key literature to provide an overview of existing home security systems, their sensors, and technologies. A comparative analysis is also carried out to identify gaps in current research and highlight areas with potential for further investigation, including improvements in home security systems.

2.2 Related Works

Due to the extensive scope of IoT research, various studies have addressed gaps yielding varying levels of success in this field. To contextualize authors Taiwo and Ezugwu [11] proposed the iHOCS system, an intelligent home control and security system that provides a convenient and remote way for owners to control and supervise their electrical appliances using a mobile app. The system also includes a security monitoring component that uses a PIR sensor and camera to detect motion and take pictures. The authors proposed using a support vector machine learning algorithm to prevent false positives by recognizing the occupants in the snapshot taken by the camera. The system has several advantages, such as significantly reducing false positives and notifying the owner through an application and email. However, there are several limitations to the system, including the potential for random triggering of the PIR due to temperature changes, the need for adequate training of the machine learning algorithm, and the absence of a redundancy plan in the event of a power outage. Therefore, while the iHOCS system offers several benefits, areas still require improvement and careful consideration.

The proposed system by Taryudi et al. [12] for safety monitoring and home security has several advantages and limitations. One of the system's main advantages is its ability to detect and monitor various environmental factors, such as temperature, humidity, rain, and flames, which can help prevent potential hazards. The two-layer identification system, which includes an RFID card and numerical PIN code on the front door, adds an extra security layer to identify genuine users. Furthermore, the non-intrusive nature of the system means that the owner will not be disturbed while at home, and the system

is activated. However, there are also some limitations to the proposed approach. For instance, the system cannot differentiate between pets and intruders, which may lead to false alarms. Additionally, the inability to track intruders' movements may make it challenging to monitor or locate an intruder in case of a security breach. Finally, the lack of a redundancy plan in case of a power outage may affect the system's reliability and pose a potential safety risk. Therefore, it is crucial to address these limitations to ensure the effectiveness and reliability of the proposed method.

Ramli et al. [13] propose a novel security system that avoids the limitations of the PIR sensor by utilizing load cells to detect the weight of an intruder. The load cells are placed behind tiles; the sensor can determine their weight if a person steps onto them. The weight threshold of 30 kg is set to avoid detecting animals and trigger alerts in real-time. The system allows tracking of the intruder's movement and is non-intrusive. However, the system requires many load cells, and an object falling on the tile may trigger a false alarm. Additionally, there is no way to ensure the detected entity is genuinely human. Furthermore, the load cell system's complexity and the need for a cable connection to an Arduino connected to the Wi-Fi network may increase the system's cost and installation complexity. Therefore, while the load cell system presents a promising alternative to the PIR sensor, further research is needed to improve its accuracy, reliability, and practicality for home security applications.

Das and Neelanarayan [14] proposed an anti-theft system for shops using a PIR sensor and camera. The system is manually activated when the shop is empty. The PIR sensor detects infrared radiation and triggers the camera to take a picture for face recognition. If the face is unrecognized, an alarm is triggered, and the owner is notified. One of the advantages is that the system provides a backup plan in case of a blackout, ensuring that the system can continue to operate uninterrupted. Additionally, the system can distinguish between employees and intruders using facial recognition technology, which enhances security. However, there are also some drawbacks to the approach. For example, false positives may occur if the camera fails to capture the intruder's face accurately. Furthermore, passers-by may trigger the PIR sensor unnecessarily, leading to false alarms. Finally, although the paper claims an accuracy rate of 75%, the system was tested on image datasets and not real-life footage, which raises questions about its real-world performance.

Dorothy et al. [15] present a unique approach to home security by using a reed switch and a camera to detect and capture images of intruders. The system's ability to minimize power consumption by sending complex processing to the fog and taking fewer images is commendable. However, the system's cost is a significant disadvantage, as a reed switch and camera are required for each door, and there is no solution for blackouts. Furthermore, the system's sole method of alerting the owner when there is an intruder may not be sufficient, as it may be easy to miss the alert. Overall, the proposed security system presents a promising solution to home security, but improvements are needed to address the system's limitations.

The proposed security system by Sivarathinabala et al. [16] is based solely on cameras, which can identify an occupant based on their face and gait. It continuously records video footage from two cameras installed at specific locations, which are then processed by a computer algorithm to identify occupants. An alarm is triggered if an intruder is

detected. The system is advantageous because it can recognize occupants, and alarms are only activated for humans, not pets. Additionally, the intruder can be tracked as there are cameras in opposite directions, and when the alarm is triggered, it is almost sure that there is a person. However, the system has several disadvantages, including high power consumption due to continuous monitoring and processing and the requirement of high resources for processing. Furthermore, the approach is not practical if there is a power cut. Additionally, it is intrusive, and the owner can feel like they are losing their privacy. Finally, the positioning of the cameras is critical for system efficiency, which can be challenging to achieve.

The above studies have proposed different approaches for IoT-based home security systems, each with advantages and limitations. Taiwo and Ezugwu [11] proposed the iHOCS system, which uses a support vector machine learning algorithm to prevent false positives and includes a security monitoring component. Taryudi et al. [12] proposed a safety monitoring and home security system that can detect various environmental factors but cannot differentiate between pets and intruders. Ramli et al. [13] proposed a security system that uses load cells to detect the weight of an intruder but requires many load cells and has installation complexities. Das and Neelanarayan [14] proposed an anti-theft system for shops using a PIR sensor and camera, but real-life footage testing limitations exist. Dorothy et al. [15] proposed a home security system using a reed switch and a camera, which minimizes power consumption but has a high cost and no solution for blackouts. Sivarathinabala et al. [16] proposed a camera-based security system that can recognize occupants and track intruders but has limited coverage and requires a clear view of the cameras.

2.3 Comparative Analysis

The related works discussed have been compiled in Table 1. Each paper presents a distinct approach to securing homes from intruders using various sensors, algorithms, and technologies. The papers have been categorized based on their detection mechanisms, such as image processing, sound, and weight detection. A comparative analysis of the different approaches has been provided by summarising each paper's proposed system, advantages, and limitations.

3 Design and Development

This study aims to design a home security surveillance system with a floor detection mechanism to prevent unauthorized access. The floor mat will consist of a sensor array configured in a matrix to detect varying degrees of pressure. When the mat detects pressure, a camera will initiate recording to identify human presence. A Convolutional Neural Network (CNN) model will be employed to optimize accuracy and functionality on low-resource devices. This section provides a walkthrough of the various steps that entailed the development of the proposed system.

Table 1. Taxonomy of the Related Work

Security System	Identification Method	Sensors Used	Advantages	Disadvantages
Taiwo and Ezugwu, 2021	Machine learning algorithm to differentiate between occupants and intruders	PIR sensor, camera	Significantly reduces false positives, remote control, notifications via app and email	PIR may be triggered randomly, training the machine learning algorithm is time-consuming, no redundancy plan
Taryudi et al., 2018	RFID card and numerical PIN code on the front door	PIR sensor, flame, rain, temperature, humidity	Flame detection, two layers of identification, non-intrusive	Cannot differentiate between pets and intruders, no tracking or monitoring of intruders, no redundancy plan
Das and Neelanarayan, 2020	Face detection	PIR sensor, camera	Provides backup in case of power cut, can recognize employees from intruders	Positioning of camera is critical, PIR may be triggered unnecessarily, and accuracy not tested on real-life footage
Dorothy et al., 2017	Image processing to detect intruders	Reed switch, camera	Complex processing done in fog, fewer images taken than with PIR	Expensive, no solution for power cut, and only one method to alert the owner
Sivarathinabala et al., 2019	Face and gait recognition	Two cameras	Can recognize occupants, alarms triggered only for humans	Requires two cameras, may not work well in low light conditions
Ramli et al., 2021	Floor detection	Load cells	Intruders cannot bypass the system easily, and it allows tracking	Requires many load cells and risk of false alarm if an object falls on tile. Cannot be sure if detection is from a human

3.1 Methodology

The development of the security system utilized a prototyping methodology, where an initial prototype was constructed and tested against the initial requirements. Through the testing process, design issues were promptly detected and resolved, allowing for the continuous refinement of the prototype until a final design was achieved that met all requirements. This methodology detected and resolved issues early in the development process, saving time and resources while delivering a high-quality security system. The mat algorithm was also refined and adjusted based on the test results to optimize the detection.

3.2 Design

To create the monitoring device, it is necessary to assemble various hardware components, including sensors, and connect and program them to meet the system requirements. The design architecture of the system is shown in Fig. 1.

The sensor used to build the mat is a piezoresistive sensor. This type of sensor is affordable, widely available on the market and can be integrated easily into an electronic circuit. The sensors will be arranged in an $n \times n$ matrix to enable tracking features. Each cell in the matrix will correspond to a location on the carpet, and the pressure applied to adjacent cells will reveal the intruder's position. An Arduino will be connected to the mat and will continuously send the pressure values of each sensor wirelessly to a Raspberry Pi for monitoring. The design is represented in Fig. 2 (a).

The Raspberry Pi will collect the sensor data and then process them using standard deviation statistical analysis to determine if an object is on it. A signal is transmitted to activate the camera to ascertain whether the object is human. The camera captures five image frames of the surroundings for one second, and a trained CNN algorithm processes each image to detect human presence. If most of the frames indicate the presence of an intruder, the picture is saved, and bounding boxes are added around the burglar. Then, it is sent to the owner by email. The latter is also notified of the intrusion by SMS using the GSM network. The pressure values are also sent to a web application where the intruder's location on the mat can be observed.

To ensure uninterrupted operation, the Raspberry Pi will be equipped with a battery to sustain the system during blackouts. In the event of a power cut, the controller will take note of the internet connection loss and store the time and date in a log file. Once the internet connection is restored, the system will notify the owner of the power outage and upload information on the duration of the blackout to the online database. As long as there is enough battery power, the device will continue monitoring. However, without an internet connection, the owner will receive SMS notifications. Nevertheless, the system will record incidents locally and upload them to the online database once the internet connection is re-established. The design of the Raspberry Pi is represented in Fig. 2 (b).

3.3 Development

The material used to develop the mat is the Velostat. Velostat is an electrically conductive plastic film with piezoresistive properties, changing its electrical resistance in

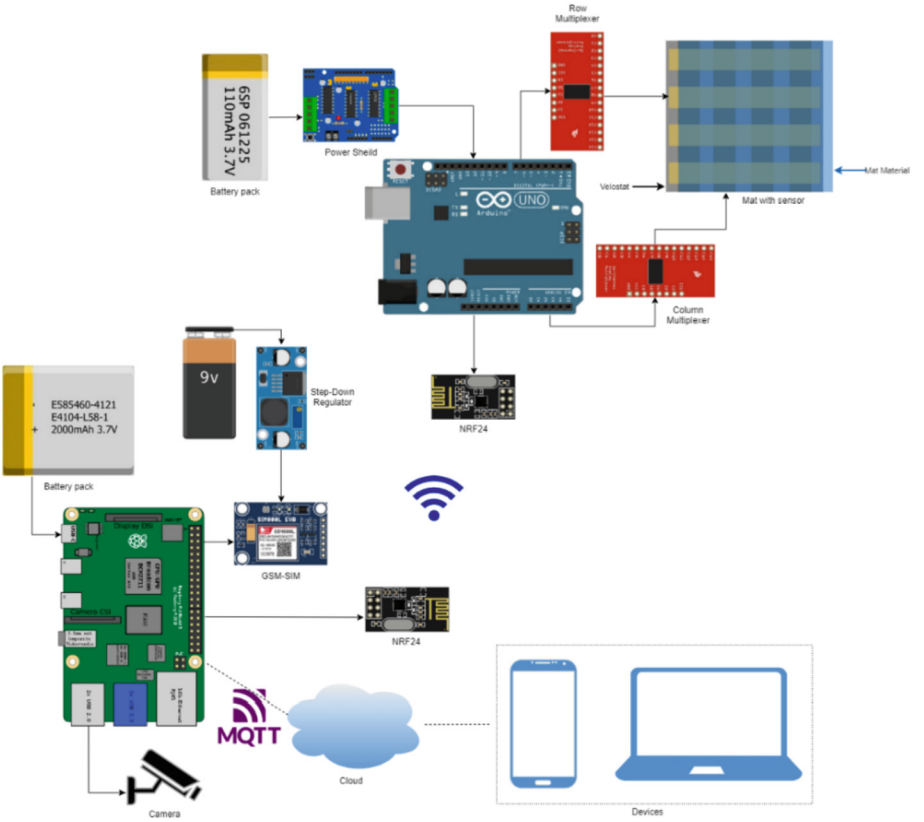

Fig. 1. Design Architecture

response to pressure or deformation. Hopkins et al. [17] briefly discussed the different applications for using this material, such as in human movement monitoring and finger gesture recognition.

The mat was built with a similar design as in the study of [18]. To achieve this, two 16-channel analogue multiplexers were implemented, with one managing signal transmission to the columns on the mat while the other was responsible for reading values from the rows. For the rows and columns, copper tape and aluminium were utilized as conductive materials. However, the copper tape was only available in a 5 mm width, and to increase this to 20 mm, it was paired with aluminium tape. Copper tape was preferred over aluminium tape for attaching ribbon cables, as it was easier to solder onto. Figure 3 shows the layout of the mat used for construction. The other materials used can be found in Table 2.

The pressure data collected from the mat was transmitted wirelessly to the Raspberry Pi via the Nrf24L01 operating on the 2.4 GHz frequency band. Subsequently, several analyses were conducted on the data to determine the presence of an individual on the mat. Statistical analysis, singular value decomposition, and eigenvalues were computed from the pressure values. The investigation results indicated that the standard deviation

(a). Arduino connected to Mat Sensor

(b). Connection of Raspberry Pi

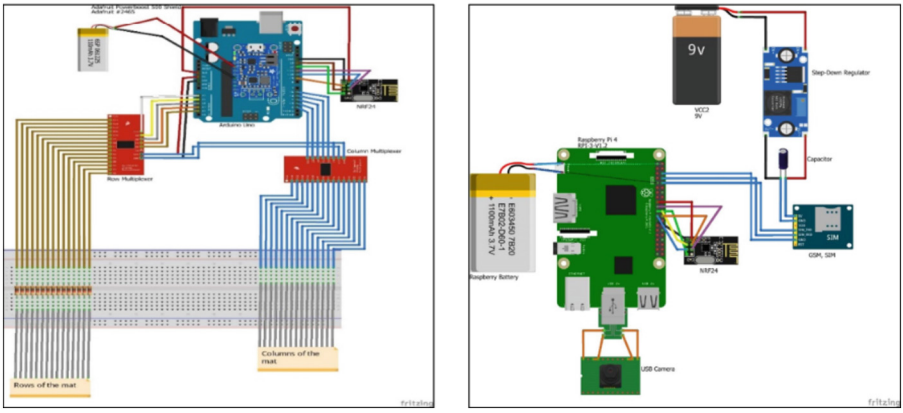

Fig. 2. Connections of the Arduino to the mat sensor

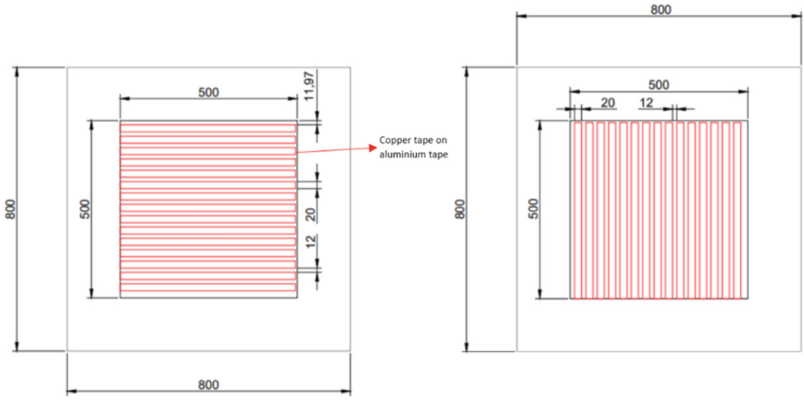

Fig. 3. Construction of the Mat

method produced more satisfactory outcomes when compared to other techniques. Thus, it was selected as the preferred approach and calculated using Eq. (1). The results of the standard deviation method, when an individual walked on the mat, were graphically represented and presented in Fig. 4.

$$\sigma = \sqrt{\frac{\sum_i \sum_j \left(x_{ij} - \mu\right)^2)}{nm}} \tag{1}$$

The CNN algorithm employed in this study utilized Tensorflow Lite in conjunction with the EfficientNet model. This particular model was selected based on research conducted by Isuyama and Albertini [12], who demonstrated its superior accuracy in object classification, achieving an impressive 94% while exhibiting reduced memory usage

and size compared to other models. Consequently, the EfficientNet model is the most appropriate for utilization on limited-resource devices such as a Raspberry Pi.

A web application was developed to provide interactive functionality with the security system, enabling real-time monitoring of the intruder's location on the mat. Communication between the device and the web application was facilitated using the MQTT protocol, which a publish/subscribe model characterizes. Specifically, the device published pressure values, and the web application subscribed to the corresponding topic. The pressure values were subsequently processed into colour representations and utilized to update the heatmap on the webpage, resulting in a tracking mechanism for locating the intruder on the mat. The web application also logs past intrusions and the history of blackouts with their dates and duration.

Fig. 4. Graphical Representation of Standard Deviation of Pressure Values

Table 2. Hardware Used in the System

Device	Model	Use
Raspberry Pi	Pi 4 Model B	The brain of the system. It processes the data received from the mat and activates the camera when needed. It also sends notifications to the user
Arduino Uno	ATmega328P 16 MHz	Reads pressure values from the mat and sends them to the Raspberry Pi
Uninterrupted Power Supply	PiJuice with 1820 mAh battery	Provide backup when there is no electricity to keep the system running
Radio Transceiver	Nrf24L01	Transmits & receives pressure values
Camera	C922 Pro	Takes pictures, which will be processed
Cellular Module	SIM800L Version 2	Sends SMS via the GSM network

4 Testing

An appropriate testing environment was established to validate the monitoring device's efficacy. The camera was strategically positioned to cover a significant portion of the room, with a clear line of sight to the intruder as they traversed the mat. Multiple test cases were conducted to evaluate the performance of the detection system, ensuring that it functioned under the anticipated specifications. The test cases are elaborated on in Table 3.

Table 3. Test Cases Performed on the System

ID	Test Cases	Description	Expected Behaviour	Pass
01	Human on the mat and in camera's vision	Humans of weights from 40 kg to 75 kg walked normally on the mat	The system should activate, detect the intruder, and alert the owner	Y
02	Human on the mat but only half body in camera's vision	Humans walk on the mat and activate the system, but only half of the body is in the camera's vision	The system should activate, detect the intruder, and alert the owner	Y
03	A non-human object on the mat	An arbitrary object of 2 kg is placed on the mat to activate the system	The system should activate but not alert the owner	Y
04	Both human and non-human objects on the mat	An arbitrary object is already on the mat. Then a human walked on it	The system should detect changes in pressure when an intruder walks on the mat and alert the owner, even if other objects are already on it	Y
05	A second mat is added to the system	Since pressure values are sent wirelessly to the Raspberry Pi, a second mat should be easily added, and the system should be able to process the values between the two mats	The system should be able to differentiate between the pressure values of the two mats and alert the owner of the exact location	Y

The system's responsiveness has also been assessed by measuring the duration between a human's detection and the owner's notification. Specifically, the instances when an object is initially detected when the system confirms the object as a human and when all the alerts are sent, and the database is updated have been recorded across fifteen trials. Table 4 presents the collected data on detection and notification times in seconds. Results show that the system exhibits an average detection time of 2.3 s and an average notification time of 12.8 s, encompassing SMS and email alerts and intrusion logging into the database.

Table 4. Responsiveness of the System

Tests	Detection Time (s)	Notification Time (s)
1	2.495529175	11.88773441
2	2.20410347	12.83382773
3	2.167779207	13.64314818
4	2.358976134	12.99078451
5	2.100421437	13.28403222
6	2.425074197	12.22190557
7	2.288811947	13.1683855
8	2.048316234	12.42726934
9	2.175364766	13.00719492
10	2.352291611	12.49614017
11	2.195211182	12.33180342
12	2.109123326	13.2607751
13	2.484581985	12.54253524
14	2.379875462	13.49991129
15	2.527416902	11.99954764
Average	**2.289137284**	**12.78823678**

Based on the results of 15 tests conducted, the system demonstrated a 100% detection rate and a 0% false positive rate in detecting intruders. The system's low false positive rate can only be attributed to its activation when pressure is applied to the mat, followed by confirmation via the CNN EfficientNet model. However, according to Liu [19], the EfficientNet model has an accuracy of 80.4%. Therefore, the system's overall accuracy is also 80.4%, as the detection depends on the vision model's performance.

5 Evaluation and Results

The developed home monitoring system was evaluated in terms of meeting the initially defined requirements. A comparative analysis has also been conducted with major related works to assess the uniqueness and distinctiveness of the system. Furthermore, the system's strengths and limitations are analyzed to evaluate the security system comprehensively.

5.1 Functional Requirements

(See Table 5).

Table 5. Fulfilment of the Requirement

Functional Requirement	Fulfilled?	Remarks
Correct identification of a human intruder	Yes	The system utilizes the TensorFlow framework with the EfficientNet model to detect human presence on the images captured by the camera when an intruder steps on the mat
Immediate owner notification	Yes	The system employs two notification channels to alert the owner of an intrusion. The average time taken to notify the owner is 13 s
Blackout resistance	Yes	The device is equipped with a battery that provides power during a power outage, enabling the device to function continuously during a blackout. The current battery capacity permits the device to operate for up to one hour
Intrusion and blackout logging	Yes	The device records the date and time of each intrusion and power outage in an online database accessible through the web application. When an intrusion occurs, the image of the intruder is uploaded to the database. The blackout duration is calculated and logged when there is a power cut

5.2 Comparative Analysis with Related Works

(See Tables 6 and 7).

Table 6. Comparative Analysis of Existing Research

Characteristics	Developed Security System	Taiwo and Ezugwu, 2021	Taryudi et al., 2018	Das and Neelanaray an, 2020	Dorothy et al., 2017	Sivarathi-nabala et al., 2019	Ramli et al., 2021
Non-avoidable	Yes	No	No	No	Partially	Yes	Yes
Human detection	Yes	Yes	Yes	Partially	Yes	Yes	No
Non-intrusive	Yes	Yes	Yes	Yes	Yes	No	Yes
Tracking	Yes	Partially	No	Partially	Partially	Yes	Yes
Redundant Notification	Yes	No	No	Yes	No	No	No
Powercut- resistant	Yes	No	No	Yes	No	No	No

5.3 Analysis of Developed System

Table 7. Analysis of the Developed System

Strengths	Limitations
Remote activation and deactivation	No notification in areas without mobile network
Accurate detection of human intruders	Ghost values may appear on the heatmap
Dual notification channels	Occasional disconnection from the mat sensor after intrusion
Unintrusive and real-time monitoring	No preventive action is taken against burglars
Scalability	The web application does not know when the device is offline
Blackout resistance	Latency issue on the heatmap during the human detection process
Log of intrusion and blackout history	Due to the complexity entangled with other parts of the system, the mat hardware alone could not be further tested

6 Conclusion and Future Works

The project has successfully developed a home security monitoring system that utilizes a flooring detection mechanism sensor. The system addresses the limitations of traditional security systems that rely on passive infrared sensors, which can be easily bypassed. The proposed method uses a low-cost piezoresistive material, Velostat, to create a matrix of 225 sensors that can track an intruder's location on the floor and determine whether it is a human. The system also incorporates a camera and a CNN algorithm using the EfficientNet model to confirm the presence of a human intruder. Furthermore, the system provides redundancy and is blackout-resistant, making it a reliable security solution for homeowners.

Future research can focus on developing more sophisticated algorithms that can detect and classify multiple intruders and homeowners to prevent false alarms. Other suggestions for future works include creating a separate thread for sending pressures to the web app to prevent latency during an intrusion, developing a mobile application to complement the web app, enhancing communication protocols between the RPi and Arduino to reduce packet loss, and researching the simultaneous increase of inter-distance on both top and bottom layers for better results. Overall, the developed prototype can serve as a foundation for further research and development of advanced home security monitoring systems.

References

1. Hoque, M.A., Davidson, C.: Design and implementation of an IoT-based smart home security system. IJNDC **7**(2), 85 (2019). https://doi.org/10.2991/ijndc.k.190326.004

2. Surantha, N., Wicaksono, W.R.: Design of smart home security system using object recognition and PIR sensor. Procedia Comput. Sci. **135**, 465–472 (2018). https://doi.org/10.1016/j.procs.2018.08.198
3. 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. (2022). https://doi.org/10.1007/s10209-022-00937-0
4. SafeHome.org Research, "Home Security Statistics in 2021," SafeHome.org (2021). https://www.safehome.org/data/home-security-statistics/. Accessed 21 Sep 2022
5. Gonzalez, M.: Reducing false alarms with AI and deep learning (2022). https://www.security101.com/blog/reducing-false-alarms-with-ai-and-deep-learning. Accessed 21 Sep 2022
6. Doan, T.T., Safavi-Naini, R., Li, S., Avizheh, S.K.M.V., Fong, P.W.:Towards a resilient smart home. In: Proceedings of the 2018 Workshop on IoT Security and Privacy, pp. 15–21. ACM, Budapest Hungary, August 2018. https://doi.org/10.1145/3229565.3229570
7. Tholen, C.: If the Power Goes Out, Does My Security System Still Work? SafeWise, 12 April 2021. https://www.safewise.com/home-security-faq/do-security-systems-work-power-out/. Accessed 21 Sep 2022
8. Desnanjaya, I.G.M.N., Arsana, I.N.A.: Home security monitoring system with IoT-based raspberry Pi. IJEECS **22**(3), 1295 (2021). https://doi.org/10.11591/ijeecs.v22.i3.pp1295-1302
9. Sharma, M., Assotally, A., Bekaroo, G.: RaspiMonitor: a raspberry pi based smart home monitoring system. In: 2022 3rd International Conference on Next Generation Computing Applications (NextComp), pp. 1–6. IEEE, Flic-en-Flac, Mauritius, October 2022. https://doi.org/10.1109/NextComp55567.2022.9932198
10. Ring, "Ring Alarm Pro," Ring. https://ring.com/products/alarm-pro-base-station. Accessed 19 Mar 2023
11. Taiwo, O., Ezugwu, A.E.: Internet of things-based intelligent smart home control system. Secur. Commun. Netw. **2021**, 1–17 (2021). https://doi.org/10.1155/2021/9928254
12. Adriano, D.B., Budi, W.A.C.: IoT-based integrated home security and monitoring system. J. Phys. Conf. Ser. **1140**, 012006 (2018). https://doi.org/10.1088/1742-6596/1140/1/012006
13. Binti Ramli, R., Binti Nazri, N.D.A., Al-Sanjary, O.I., Rozzani, N.: The development of weight detection system using IOT flooring. In: 2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), pp. 250–255. IEEE, Penang, Malaysia, April 2021. https://doi.org/10.1109/ISCAIE51753.2021.9431787
14. Das, S., Neelanarayan, V.: IoT Based Anti-Theft Flooring System, p. 4 (2020)
15. Dorothy, A.B., Kumar, S.B.R., Sharmila, J.J.: IoT based home security through digital image processing algorithms. In: 2017 World Congress on Computing and Communication Technologies (WCCCT), pp. 20–23. IEEE, Tiruchirappalli, Tamil Nadu, India, Feburary 2017. https://doi.org/10.1109/WCCCT.2016.15
16. Sivarathinabala, M., Abirami, S., Deivamani, M., Sudharsan, M.: A smart security system using multi-modal features from videos. Pattern Recognit Image Anal. **29**(1), 89–98 (2019). https://doi.org/10.1134/S1054661819010218
17. Hopkins, M., Vaidyanathan, R., Mcgregor, A.H.: Examination of the performance characteristics of velostat as an in-socket pressure sensor. IEEE Sens. J. **20**(13), 6992–7000 (2020). https://doi.org/10.1109/JSEN.2020.2978431
18. Kumar, V., Yeo, B.-C., Lim, W.-S., Ra, J.E., Koh, K.-B.: Development of electronic floor mat for fall detection and elderly care. Asian J. Sci. Res. **11**(3), 344–356 (2018). https://doi.org/10.3923/ajsr.2018.344.356
19. Liu, R.: Higher accuracy on vision models with EfficientNet-Lite (2020). https://blog.tensorflow.org/2020/03/higher-accuracy-on-vision-models-with-efficientnet-lite.html. Accessed 30 Sep 2022