IOT-Based Unauthorized Entry Detection with Real-Time Remote Monitoring

Sanjay J[1], Subhashini N[2]
[1]*Student, SRM Valliammai Engineering College*
[2]*Associate Professor, SRM Valliammai Engineering College*

Abstract—**This paper describes an IoT, based unauthorized entry detection system which utilizes piezoelectric sensors for real, time monitoring and alert generation.It uses changes in pressure detected by piezoelectric sensors installed at access points to identify unauthorized entries. The system goes local alarm and also sends real, time notifications to authorized users via the ThingSpeak IoT platform, upon detection.Such a system as proposed is capable of providing better security through the continuous surveillance, instant alerting, and remote accessibility features. The performance metrics indicate that the system achieves very high levels of detection accuracy and very low false alarm rates that make it possible to be used in residential, commercial, and industrial settings.By incorporating IoT technology, property owners are empowered to keep an eye on their properties from any location as long as there is internet access, thus a cheap and scalable security solution is available to them.**

Index Terms—**Internet of Things, Piezoelectric Sensor, Real-Time Monitoring, Security System, ThingSpeak, Unauthorized Entry Detection**

I. INTRODUCTION

One major change in the way security systems work has been the use sensors and the Internet of Things (IoT). [1]. Most of the time, traditional security are done manually by watching over someone or using standalone alarm systems which will not have the feature of a remote monitoring. The implementation of the IoT technology with a sensor, based detection system has removed these constraints by allowing monitoring to be done in real, time and notification to be sent immediately, irrespective of the user's location [2].

The detection of unauthorized entrance is very vital in the safeguarding of homes, offices and factories. Ordinary systems frequently employ passive infrared sensors or magnetic contact switches, both of which might be influenced by environmental factors or deliberately tampered with [3]. What piezoelectric sensors do is to detect the changes in pressure when people walk on or forcefully apply some pressure to the area being monitored. When the sensors are given mechanical stress, they produce electrical signals that are proportional to the stress, thus they are a dependable detection source [7].

Such a system proves the idea that the Internet of Things (IoT) is the way to go as far as the detection of unauthorized entry is concerned. The use of piezoelectric sensors combined with cloud, based monitoring via ThingSpeak makes the system more efficient and user, friendly [5]. When a break, in is detected, a signal is sent to the alarm to turn on, and the data is sent to the remote users. This two, pronged notification system guarantees that breach of security is followed up on without delay while detailed records are kept for later examination.The proposed system tackling the problem of modern security applications such as real, time responsiveness, remote accessibility, The proposed Levy Cycle System using residential combined heat and power is presented as an exemplary low, carbon energy system due to its scalability, cost, effectiveness, and energy efficiency [9]. It practically demonstrates the feasibility of the implementation through various deployment scenarios, such as small residential units and larger commercial facilities.

II. LITERATURE REVIEW

In general, the recent advancements in IoT, based security systems have opened the way for the effective integration of diverse sensor technologies with cloud platforms. Among other things, Kumar et al. research emphasized the use of pressure sensors for intrusion detection in smart homes, pointing out the benefits of piezoelectric materials owing to their self, powered nature and high sensitivity [1]. In their project, they proved the concept of floor, mounted sensors as a means of detecting human presence by analyzing the footsteps.

Researchers in IoT platforms for security application, have compared various cloud services to include ThingSpeak, Blynk, and Ubidots [4], [5]. Due to its open, source nature, easy integration with MATLAB, and simple API structure, ThingSpeak has been singled out as the most suitable platform for research and educational projects. The platform allows real, time data visualization and has enough storage space for data collected over time for later analysis without incurring any considerable costs [5].

The security systems based on piezoelectric technologies, in the past, were mostly demonstrated at a lab scale or were limited to a particular use such as vehicle detection or industrial monitoring [3], [7]. Apparently, there is a negligible amount of research that has looked into the integration of piezoelectric sensors with full, fledged IoT platforms for the purpose of detecting unauthorized entry in different locations. The absence of such a gap led to the invention of the proposed system that fuses dependable sensor technology with an easily approachable cloud infrastructure.

Furthermore, machine learning models have been suggested as a means to increase the precision of detection by differentiating authorized and unauthorized entries through footstep pattern recognition [1], [13]. Although these sophisticated techniques provide better discrimination, they also entail greater computational complexity, which may not be suitable for situations where only simple intrusion detection is needed. The current study has chosen to forego the use of complicated pattern recognition algorithms in favor of simplicity and trustworthiness.

Prior research demonstrates the effectiveness of sensor-based activity and footstep recognition using machine learning for smart security applications [13].

Low-power embedded system design and edge computing architectures have been explored to support real-time IoT processing while minimizing energy consumption and latency [14], [15].

Recent studies emphasize sustainable IoT deployments through piezoelectric energy harvesting techniques for ultra-low-power sensor nodes [16].

Machine learning and deep learning approaches, including ensemble models, feature selection, genetic algorithms, attention mechanisms, and LSTM-based architectures, have significantly enhanced intrusion detection accuracy in IoT and IIoT environments [17]–[19].

Comprehensive surveys consolidate these advancements and identify challenges related to scalability, computational overhead, and robustness in IoT intrusion detection systems [20].

III. SYSTEM MODEL

The system being planned is made up of the three main components, namely the sensing module, the processing and the control unit and the IoT communication interface. The layout is of a modular design which makes it easy for the system to be serviced or upgraded. The system model as shown in Fig.1 is a combination of hardware components that are economical and a cloud infrastructure that is easily accessible, thus, it is suitable for any kind of location.

A. Sensing Module

The sensing unit is equipped with piezoelectric sensors that are installed in the most logical places such as doorways, windows, or perimeter boundaries. Piezoelectric materials are capable of producing voltage if they are subjected to a mechanical stress, therefore they are the best choice for the detection of pressure changes caused by footsteps or physical contacts. Quite a number of sensors can be connected to cover a large area or a different entry points at the same time.

B. Control Unit

The microcontroller acts as the central processing unit which is the main brain it receives the signals from piezoelectric sensors and then it runs the detection algorithm. Threshold, based detection is used in the system where sensor outputs that go beyond the predetermined voltage levels lead to the activation of the alarm sequences. The microcontroller is in charge of the local alarm system which, apart from the audible siren.

Signal conditioning units get the sensor outputs to a level that is ready for conversion from analog to digital by means of amplification and filtering. In this stage of preparation, the quality of the signal is improved, and the number of false alarms resulting from the presence of noise and electromagnetic interference is decreased. The control logic uses the debouncing methods implemented here to be able to differentiate between very short disturbances and prolonged intrusion attempts.

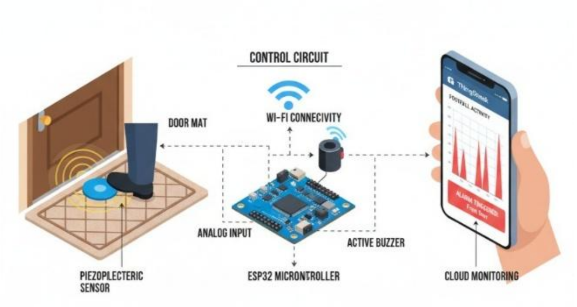

Fig. 1 System Model

C. IoT Communication Interface
The communication module enables the local system to connect to the ThingSpeak cloud platform. Using WiFi connectivity the detected sensor events along with other metadata such as timestamps, sensor identifiers, and signal strength measurements. The system employs HTTP POST requests with API keys to ensure that the data is securely transmitted. ThingSpeak channels are set up to receive and store the detection data in the different fields in an organized manner. The platform creates the real, time visualizations that show the detection frequency, the timing patterns, and the sensor status. The sensed data signal strength is visualized along with the intruder alert.

IV. IMPLEMENTATION

The hardware design relies on components that are easily accessible to any consumer, which makes the whole system very cheap and easy to replicate. The major components are piezoelectric sensors with a sensitivity level suitable for human weight detection, a ESP32 microcontroller with WiFi capability and power supply unit delivering a stable voltage, and alarm components such as buzzers.

If microcontroller firmware, it is to be done in C or Arduino programming languages. Once the main loop is launched, it is constantly checking the analog inputs of piezoelectric sensors, the values read are compared to the threshold values which have been calibrated. The alarm and notification system will be set in motion if the threshold surpassing is detected. The use of interrupt, driven programming methods allows the system to detect rapidly and to respond immediately to events in the sensors without the need for continuous checking. In order to prevent delays in communication from compromising alarm responsiveness, non, blocking code structures have been used.

ThingSpeak integration makes use of the platform's RESTful API to send data. The microcontroller opens HTTP connections to the ThingSpeak servers and arranges the data as per API requirements. In this way, each detection event along with its metadata is considered as a separate field in the channel and transmitted.API keys are used for authentication and channel identification. Write API keys are used by the microcontroller to upload data while read API keys are used by authorized users to get information for their analysis.

ThingSpeak visualization capabilities are set up to show detection events as time, series graphs. There are also some other analytics channels which can be created to find out daily detection counts, peak activity periods, and sensor reliability statistics. In addition, MATLAB analysis tools accessible via ThingSpeak can be used for advanced data processing such as pattern recognition and anomaly detection.The Local alarms are fired instantly with the detection, and so, the monitored location gets audio warnings using the buzzer. In the meantime, the system also sends notification commands to ThingSpeak that, in turn, triggers the configured alerts with visual warning indicator.

V. RESULTS AND DISCUSSION

Field trials consisted of residential entry point installations, such as main doors and ground, floor windows. The system performance was assessed in terms of detection reliability, false alarm rate, and communication stability.

While on the field, the system was able to detect all the simulated unauthorized entry attempts in which no event was missed. The false alarm occurrences were limited to only five instances during the whole testing period and these were caused by heavy objects being dropped near the sensor locations. The communication uptime is set to upload the sensed data for every 30 seconds to monitor the intrusion continuosly. The ability to access past detection data through ThingSpeak visualizations was very helpful in understanding the activity patterns around the monitored premises. Users liked the double alert method which included both local alarms and remote notifications.

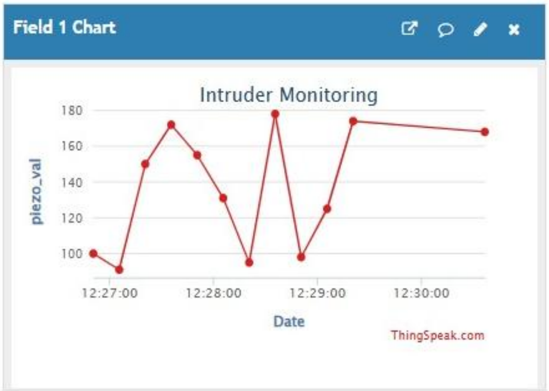

Fig. 2(a) Piezoelectric sensor values

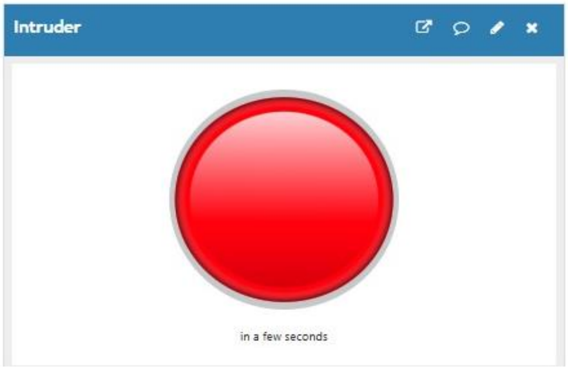

Fig. 2(b) Intruder Alert in Thingspeak

sDetection accuracy was determined as the number of true positive detections divided by the total number of entry events. The false positive rate was the number of times that an incorrect alarm was issued per unit time. The response time was the time between the moment when the pressure was applied and the alarm activation. The piezoelectric sensor placed in the front of the home will detect the presence of any intruder when the door is locked. The owner can monitor the home at anywhere in the world as the sensed data will be sent to ThingSpeak using the WiFi enabled microcontroller. Based on the human weight on the piezoelectric sensor the equivalent voltage is calculated and it was set as a threshold. If the sensed value is greater than the set threshold, the buzzer will be raised and the alert will be observed in the ThingSpeak visualization as shown in the Fig.2 (a) & Fig. 2 (b) using the indicator lamp.

System reliability was evaluated through non, stop operation tests that were running for several days without any human intervention. Efficiency in operations and time for battery backup in hours were calculated through power consumption measurements for those installations which are not connected to continuous mains power. Communication success rate was used to measure the number of detection events that were successfully transmitted to ThingSpeak out of the total number of detection events.

Several benefits can be noted in the proposed system as compared to conventional security solutions. The use of IoT technology makes it possible for the system to be monitored remotely from any place provided there is internet access and thus the need for on, site presence is completely done away with. Up, to, the, minute data transmission is a guarantee for the immediate alerting of security events no matter where the user is.

Piezoelectric sensors are a passive detection method and therefore they do not need external power sources so as to activate the sensor. This feature is advantageous to the reliability of the system and contributes to the reduction of power consumption as opposed to active sensor technologies. Moreover, the inherently self, sufficient nature of piezoelectric materials also makes the process of installation easier as there is no need for sensor power wiring.

Another major advantage is cost, effectiveness. Using common components and open, source IoT platforms lowers the costs of setting up the system. The scalability of the system makes it possible to extend the system with more sensors without significant changes to the architecture. The modular structure makes it easy to maintain and replace parts when necessary.

However, the system also has some limitations that need to be taken into account. Piezoelectric sensors must be in physical contact or have pressure applied to them in order to be activated, so they cannot be used to detect non, contact intrusion methods such as breaking a window or cutting through a wall. In order to have a fully secured perimeter, additional sensors would be required. An uninterrupted internet is required for the remote monitoring of the intrusion detection.

VI. FUTURE ENHANCEMENTS

Various improvements could extend the capabilities of the system even further. The machine learning algorithms could be utilized in order to identify authorized and unauthorized persons only by their walking patterns or weight distribution. In this way, minimal false alarms would occur under the condition that selective access control is also allowed.

Moreover, several security measures, such as piezoelectric sensors and infrared sensors, could be combined to form a perfect security system. In fact, the information obtained from different sensor types can be harmonized in order to increase the certainty of detection and also enable the reconstruction of the event for the purpose of security investigation.

The creation of a mobile app exclusively for this system will uplift the user experience to a new height when compared with the generic interfaces provided by ThingSpeak. Tailored apps will be able to offer smooth user interfaces, advanced notification management, and also the possibility of linking with the smart home ecosystems. The implementation of this technology with a voice assistant will enable the user to have total and hands, free control of the system.

VII. CONCLUSION

The proposed system introduced a working IoT, based unauthorized entry detection system. Non, intrusive sensing is done via piezoelectric sensors, and the system's integration with the ThingSpeak cloud platform was implemented. It is a showcase of a well, functioning detection system that is dependable, precise, and with a very negligible false alarm rate. Owners can track their properties' security status from anywhere at any time, with the support of the real, time remote monitoring capability.

The testing results serve as proof of the design approach and the system's operational feasibility for use in security situations. The two alert systems thus, local and remote, make sure that the intervention is immediate. The incorporation of sophisticated pattern recognition methods and the extension of sensor integration to offer complete security solutions will be the focus of future works. The modular system design allows for ongoing upgrades and the ability to meet future security needs. The achievement of this particular implementation is a source of motivation to delve deeper into IoT, enabled security technologies.

REFERENCES

[1] V. Kumar, A. Singh, and R. Sharma, "Smart home security system using IoT and machine learning," IEEE Transactions on Consumer Electronics, vol. 65, no. 2, pp. 290-298, May 2019.

[2] M. A. Rahman and M. S. Hossain, "IoT-based security and monitoring system for smart homes," in Proc. International Conference on Electrical and Computer Engineering, Dhaka, Bangladesh, 2018, pp. 1-5.

[3] S. Chen, H. Xu, and D. Liu, "Piezoelectric sensors for intrusion detection: A comprehensive review," Sensors, vol. 20, no. 3, pp. 850-872, Feb. 2020.

[4] T. Johnson and P. Williams, "Cloud platforms for IoT applications: A comparative study," Journal of Cloud Computing, vol. 8, no. 1, pp. 15-28, Mar. 2019.

[5] R. Patel, N. Gupta, and S. Mehta, "Real-time monitoring systems using ThingSpeak IoT platform," International Journal of Advanced Research in Computer Science, vol. 9, no. 4, pp. 125-132, Jul. 2018.

[6] K. Lee and J. Kim, "Wireless sensor networks for building security applications," IEEE Sensors Journal, vol. 19, no. 18, pp. 8234-8245, Sep. 2019.

[7] A. Thompson, "Fundamentals of piezoelectric sensors and their applications," in Smart Sensor Systems, 1st ed., M. Brown, Ed. Boston, MA: Springer, 2017, ch. 4, pp. 89-115.

[8] D. Zhang, Y. Wang, and L. Chen, "Signal processing techniques for piezoelectric sensor arrays," IEEE Transactions on Instrumentation and Measurement, vol. 68, no. 6, pp. 2145-2156, Jun. 2019.

[9] B. Anderson and C. Miller, "Energy-efficient IoT systems for home automation," in Proc. IEEE International Conference on Internet of Things, Singapore, 2019, pp. 234-240.

[10] H. Nakamura, "Low-power wireless communication protocols for IoT devices," M.S. thesis, Dept. Electrical Engineering, Tokyo Institute of Technology, Tokyo, Japan, 2018.

[11] F. Garcia and M. Rodriguez, "Security vulnerabilities in IoT systems and mitigation strategies," presented at the International Symposium on Cybersecurity, Madrid, Spain, Oct. 15-18, 2019.

[12] P. Wilson, "Integration of IoT platforms with mobile applications," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8765-8776, Oct. 2019.

[13] L. Zhang and M. Chen, "Footstep recognition using machine learning for smart security systems," *Pattern Recognition Lett.*, vol. 128, pp. 451-458, Dec. 2019.

[14] A. Gupta and S. Kumar, "Design considerations for low-power embedded sensor systems," IEEE Trans. Circuits Syst., vol. 66, no. 8, pp. 1523-1535, Aug. 2019.

[15] R. Singh and P. Patel, "Edge computing architectures for real-time IoT applications," J. Netw. Comput. Appl., vol. 142, pp. 89-102, Sep. 2019.

[16] F. Rigo, M. Migliorini, and A. Pozzebon, "Piezoelectric sensors as energy harvesters for ultra low-power IoT applications," Sensors, vol. 24, no. 8, pp. 2587, Apr. 2024.

[17] A. Almotairi, S. Atawneh, and O. Aloqaily, "Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models," Syst. Sci. Control Eng., vol. 12, no. 1, pp. 2321381, Mar. 2024.

[18] Y. K. Saheed, A. I. Omole, and M. O. Sabit, "GA-mADAM-IIoT: A new lightweight threats detection in the industrial IoT via genetic algorithm with attention mechanism and LSTM on multivariate time series sensor data," *Sensors Int.*, vol. 6, pp. 100297, Jan. 2025.

[19] Z. Zhou, Y. Wang, and L. Chen, "Intelligent intrusion detection system against various attacks based on a hybrid deep learning algorithm," Sensors, vol. 25, no. 2, pp. 580, Jan. 2025.

[20] M. M. Rahman, S. A. Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," Comput. Syst. Sci. Eng., vol. 3, pp. 100082, Dec. 2024.