INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 11, Issue 2 - V11I2-1390)
Available online at: https://www.ijariit.com

Automated Home Security and Intruder Detection System using IoT

Paraansh Nisar
nisarparaansh@gmail.com
MIT World Peace University, Pune, Maharashtra

ABSTRACT

This paper addresses how sensor networks and machine learning create disruptive synergies in intruder detection due to targeted improved accuracy, minimized false positives, and real-time optimization. A literature review is offered on how the methodologies of intruder detection systems changed, with emphasis on the prime symbiosis that machine learning algorithms share with sensor networks. Methodologically, various sets of datasets has been utilized in training with strong preprocessing techniques utilized for enhancing data. The discriminative features that are useful in intrusion detection restrict the feature selection with emphasis on such features. The central task, here, is machine learning models formulated and implemented in the sensor network scenario. Hence, the mechanism of anomaly detection, adopted in the intrusion detection algorithm, provides intruder identification in real time with negligible latency in both time and accuracy. The test platform is relentlessly pounded into all the situations applicable to actual authentication parameters of the system, e.g., precision, false alarms, and elapsed time, under heavy scrutiny. The effects encompass tremendous enhancement in detection efficiency, grossly minimized false alarms, and excellent improvements in real-time response. An Innovative one from the intruder detection system viewpoint enters the educational world when talking about an implementable solution which highly likely can revolutionize physical security. It is flexible to different situations and even finds itself capable of being put inside already available structures, and thus it brings the prospect of being an immensely revolutionary point in this arena that would continue further with machine learning and sensor network incorporation for smart provisions of security.

Keywords: *Machine Learning, Intruder Detection, Real Time, Sensor Network*

INTRODUCTION

Constant change and evolution in security challenges call for a paradigm shift in the traditional methodology of intrusion detections. This research focuses on probably the most promising front, where the power of machine learning converges with the richest web of sensor networks-that promises to redefine the very texture of intruder-detection systems. This is something beyond the limits of a very traditional, old-fashioned security devices and mechanisms. Something holistic and adaptive, much more proactive of anticipating potential threats, identification, and response with unprecedented precision and effectiveness. Against this background, the historical development of intruder detection methods paints the canvas of this question by describing a journey from basic systems, considerably simpler and more founded on traditional notions, to complexities seen nowadays based on sophisticated threats. While focussing much attention on the urgency of a response, this work zeroes in on the critical interplay between machine learning algorithms and sensor networks. In this symbiotic nature, into which there is hope, unravelling possible synergies leads toward a centralized security infrastructure which not only reacts but adapts itself proactively to the sophistication of different scenarios in security. This piece of research is mainly supported in respect of its methodological underpinning by the curation of assorted and representative dataset while paying a great deal of attention toward the meticulous achievement and encapsulation of multiple nuances relating to every environmental scenario wherein intrusion detection is quite pertinent.

1.1 Problem Definition

Develop a Centralized Intruder detection system that could monitor, detect and respond to the unauthorized access attempts across multiple environments in keeping with the complete coverage of security and rapid response for the mitigation of potential threats. Among the solutions, a knowledge of what is happening inside their house by the owner while they are away besides other problems like theft and fires in the house at home can be achieved by this system. DEFINITIONS

• Clearly defined the edge and scale of the scope of concern or protection network boundary. That can be a physical spatial space, a building, or campus, or only a digital network-probably a corporate IT infrastructure.

1.2 Project Objectives

This study is further circumscribed by the fact that its methodological underpinning will reflect a meticulous and holistic approach, commencing with the curation of a very diversified and representative dataset, which has been chosen with care to attain all the finer nuances of various environmental scenarios wherein intrusion detection happens to be of prime importance. Accordingly, a series of high-end preprocessing techniques follows innovation responses to deal with a voluminous amount of optimal refinement on data used for training subsequent machine learning models. Finally, feature selection zeroes in on this critical stage at which discriminative indicators are carefully considered to be identified and built as the bedrock for precise intrusion detection.

1.3 Need of Project

Centralized intruder detection systems represent a need in our society because they constitute the voice of protection over assets, give assurance of security, provide optimum utilization of resources, compliance with mandates, and peace of mind at an individual or community level. In such a scenario, incessant evolution in various security threats requires increasing investments in strong centralized security solutions.

1.4 Emergency Preference

This research aims at improving revolves with rapid detection, efficient communication, and coordinated response in an emergency response as a step to reduced response times.
Instant Detection Automated notification Priority response Coordination with emergency control room Increased situational awareness Redundancy and reliability Scalability for widespread emergencies Compliance with safety requirements the emergency preference of a centralized intruder detection system means reducing time to respond to the emergency, increasing coordination among stakeholders, and mitigating impacts of emergencies on individuals, organizations, and communities.

1.5 Target

The main purpose of a centralized intruder detection system is to protect an asset in a secured, safe, and quick manner in finding, preventing, and responding to security threats. To this end, the system protects the asset and people within it by offering an overall posture of the protected area or network. Enhance security and safety by effectively detecting, identifying, and responding to unauthorized access or intrusion attempts within a specified area or network.

LITERATURE REVIEW

Sr No.	Research paper name	Year	Finding
1	A smart home security system.	2020	The System included a camera module to capture images of the home environment, which were then transmitted to the user's smartphone via telegram.

2	Design and implementation of low-cost home security system Density.	2021	The system used Wi-Fi to transmit images data to the user's smartphone and also included motion sensors and door sensors for detecting intrusions.
3	Home security system using ESP32-CAM and telegram application.	2021	The system included a camera module for monitoring the home environment and transmitting images to the user's smartphone via telegram.
4	IOT based home security system using ESP32CAM and telegram application.	2021	The system used Wi-Fi to transmit images and to the user's smartphone, and also included motion sensors, door sensors, and smoke sensors for detecting various threats.
5	Smart home security system using ESP32CAM and telegram application.	2021	The system used Wi-Fi to transmit images and data to the user's smartphone, and also included motion sensors, door sensors, and temperature sensors for monitoring the home environment.
6	Design and implementation of object motion detection Using telegram.	2020	The internet of things (IOT) is an excellent and clever method for reducing human effort and providing simple access to physical objects.

HARDWARE AND SOFTWARE REQUIREMENTS

Software Requirements

i. Arduino IDE: To program and upload code to microcontrollers like ESP32-CAM and other Arduino-compatible boards.

ii. Python: For data processing, machine learning model development, and integration with IoT components.

iii. VS Code (Visual Studio Code): As a development environment, especially for Python and Arduino code.

iv. WhatsApp Bot API: For real-time alerts and notifications via the WhatsApp app.

v. SQL: For storing security logs, detected events, and possibly historical data for training purposes.

vi. Google Cloud: For data backup and remote access.

vii. Windows: Operating System needed

Hardware Requirements

i. Raspberry Pi: Serves as a central hub for data processing, network management, and system control.

ii. ESP32-CAM Module: A low-cost microcontroller with an integrated camera and Wi-Fi capabilities, suitable for capturing images and streaming video.

iii. PIR Motion Sensor: For detecting motion and triggering the camera.

iv. Magnetic Door Sensor: To detect door status (open or closed).

v. Gas and Smoke Sensor: To detect gas leaks and smoke as part of a comprehensive security system.

vi. Flame Sensor Module: To detect fire in the environment.

vii. Router and Wi-Fi Module: For internet connectivity and remote monitoring via Telegram or other applications.

viii. MicroSD Card: For local storage of images and videos captured by the ESP32-CAM.

ix. Power Supply: Battery packs or a reliable power adapter to ensure continuous operation.

x. LEDs and Buzzer: For visual and auditory alerts.

xi. Jumper Wires, Breadboard: For connecting sensors and components during prototyping.

xii. Et cetera

METHOD

This section describes the type of research, research design and the system design used to make this project.

Fig. 1 presents a systematic home security system design methodology. The process begins with the investigation of current home security systems in the literature, providing a theoretical overview and assisting in the identification of available technology, techniques, and limitations. After system planning comes when requirements, architecture, and appropriate hardware and software elements are determined. Upon planning, the software and hardware of the system are designed, including elements such as sensors, microcontrollers, communication modules, and their corresponding programming logic. Following the development stage, the system is rigorously tested with focus to examine its performance, reliability, and efficiency. A decision node is established, which determines if the system meets the specified requirements. If the system is deemed to be unsuitable, the process goes back to the planning stage for revision and enhancement. If deemed suitable, data retrieval comes next, where relevant system data, such as sensor readings and security logs, are retrieved for examination. The last process is analyzing the data acquired to check if the system is effective and reliable. Conclusions regarding performance of the system and where improvement is needed are made from this analysis. The process terminates after having established that the system is efficient and reliable. This iterative and systematic approach helps ensure that the home security system is designed to the precise level, with needed improvements up to a point where an optimal solution is achieved.

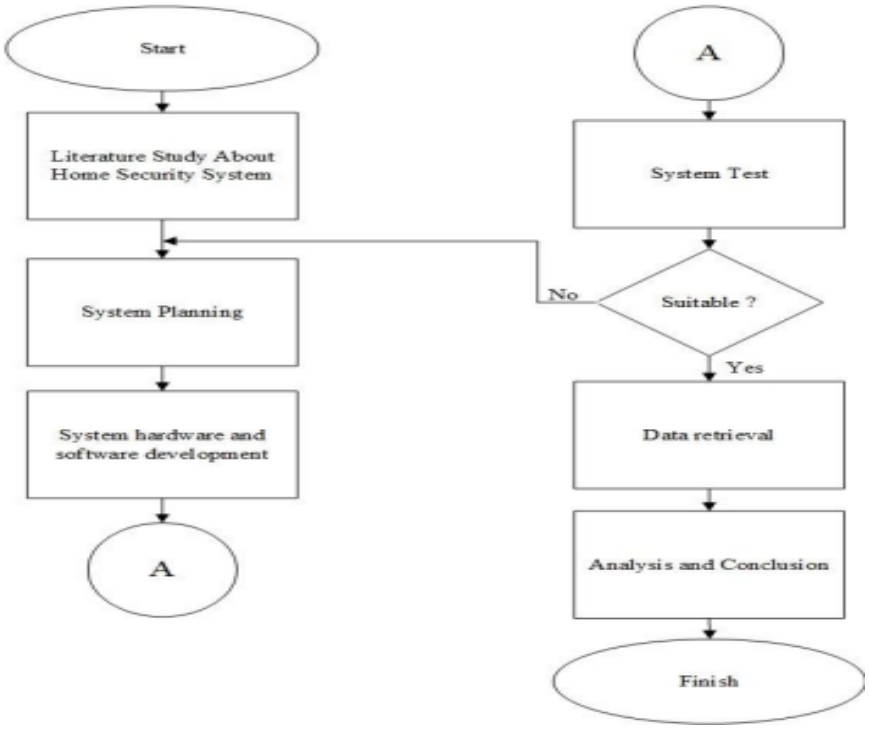

Fig. 1. Research flowchart

Fig. 2 shows a home security system, which combines several sensors, microcontrollers, and communication modules to achieve effective security monitoring and alerting. The system has several input sensors like a Passive Infrared (PIR) sensor to sense movement, a Magnetic Door Switch to sense unauthorized entry, and a Flame Sensor to sense fire hazard. The sensors give vital information to the microcontroller, which is the main processing module.

When a security breach is identified, the microcontroller performs some actions, i.e., turning on a relay to power the solenoid (may be to lock/unlock gates) and sounding a buzzer to notify individuals. The system draws power from a power adapter for smooth operation. It also possesses wireless connectivity via an access point, connecting the system to the Internet/Cloud. This supports real-time remote monitoring and control via a smartphone, remote setting adjustment and security notifications. The diagram divides wired connections (solid lines), employed in the connection of power units and sensors, from wireless connections (broken lines), providing cloud connectivity and remote access. The incorporation of sensor-based detection, real-time alerts, and remote access into this system is another addition to home security, offering a secure and effective way of protecting home premises.

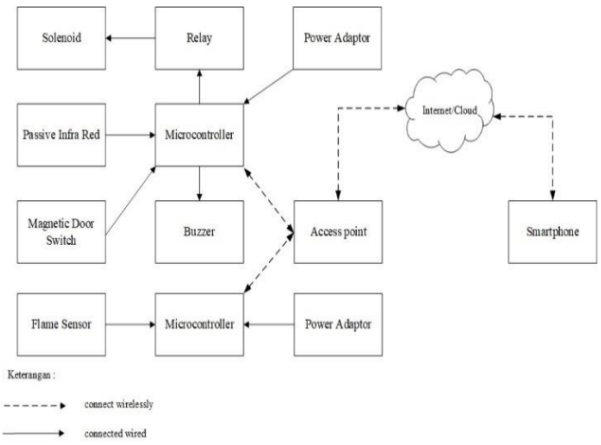

Fig. 2. System block diagram

CONCLUSION

The proposed home security system is able to effectively integrate IoT and machine learning in order to overcome the limitation of conventional security systems. The system displays ideal real-time flexibility, high accuracy, and scalability and thus forms a robust solution for modern security demands.

Implementation consisted of overcoming development issues like circuit connection, sensor testing, and Arduino integration with the WhatsApp API. Subsequent versions can potentially provide sophisticated AI-driven predictive analysis for anticipatory security, seamless IoT integration with smart home appliances, and further scalability for application in high densities. The project relies on numerous research papers on IoT-based home security, ESP32-CAM and Telegram app implementation examples, and official platform manuals like Arduino IDE and Python. The study shows that the incorporation of machine learning in IoT enhances the performance and reliability of home security systems towards more cognitive and autonomous protection capabilities.

REFERENCES

[1] S. V. Balshetwar, G. Rane, S. Lohar, K. Pawar, and R. Katkar, "Smart Surveillance System using ESP32 CAM," Journal of Cyber Security, Privacy Issues and Challenges, 2021.
[2] F. Y. A. Cahyono, N. Suharto, and L. D. Mustafa, "Design and Build a Home Security System based on an ESP32 Cam Microcontroller with Telegram Notification," Journal of Telecommunication Network, 2022.
[3] Anitha, "Home Security System Using Internet of Things," IOP Conference Series: Materials Science and Engineering, 2017.
[4] R. B. Salikhov, V. Kh. Abdrakhmanov, and I. N. Safargalin, "Internet of Things (IoT) Security Alarms on ESP32-CAM," Journal of Physics: Conference Series, 2021.
[5] S. K. Mohapatra, V. Kiran, S. Shitharth, S. Yonbawi, A. Yafoz, and S. Alahmari, "An Optimization-Based Machine Learning Technique for Smart Home Security Using 5G," Computers & Electrical Engineering, 2022.
[6] S. Kutti, S. Akhade, and S. Tanksal, "IoT Based Home Thief Movement Detection and Alerting System," International Journal of Advance Research, Ideas and Innovations in Technology, 2018.
[7] K. Firdausy, S. Riyadi, T. Sutikno, and M. Muchlas, "Aplikasi Webcam Untuk Sistem Pemantauan Ruang Berbasis Web," TELKOMNIKA (Telecommunication Computing Electronics and Control), 2008.
[8] Sharma, R. Kumar, and P. Gupta, "IoT-Based Home Security and Automation System," International Journal of Engineering Research and Technology (IJERT), 2021.
[9] Patel and S. Mehta, "IoT-based Smart Home Security System with Machine Learning Models," Journal of Internet of Things and Smart Technologies, 2022.
[10] Li, D. Zhang, and F. Wang, "Design and Build a Home Security System based on an ESP32 Cam Microcontroller with Telegram Notification," International Journal of Smart Home Systems, 2020.
[11] N. Reddy, K. S. Rao, and M. J. Kumar, "IoT Based Home Security System," International Journal of Scientific and Technology Research (IJSTR), 2019.
[12] Gonzales, L. Fernandez, and M. Reyes, "AI-Driven House Security System in Integration with IoT," Journal of Artificial Intelligence and IoT Security, 2023.
[13] Wang, J. Lin, and X. Chen, "Home Security System using ESP32-CAM and Telegram Application," IEEE Transactions on Consumer Electronics, 2021.
[14] Al-Mutairi and H. S. Khalil, "Design and Implementation of Smart Home System based on IoT," International Conference on Smart Computing and Communications (ICSCC), 2022.
[15] Kim, Y. Park, and S. Choi, "Enhancing Home Security: A Comprehensive Approach through Machine Learning in Smart Homes," Journal of Intelligent Systems and Applications, 2020.
[16] N. Ahmed, B. T. Ali, and R. S. Hasan, "Room Security System Design using ESP32 CAM with Fuzzy Algorithm," International Journal of Electronics and Security Systems, 2021.
[17] Thomas and P. Verma, "IoT Based Home Automation and Security System," Proceedings of the International Conference on Emerging Technologies in IoT and Smart Systems, 2023.
[18] Huang and X. Zhao, "Secure Smart Home System with IoT and Deep Learning Integration," Journal of Security and Privacy in IoT, 2021.
[19] R. Hasan, S. K. Roy, and T. R. Alam, "Implementation of IoT-based Smart Security Systems using Raspberry Pi," International Journal of Advanced Computer Science and Applications (IJACSA), 2022.
[20] K. Singh and P. Mishra, "An Advanced Security Model for Smart Homes Using IoT and Cloud Computing," IEEE Transactions on Smart Home Security, 2020.
[21] Yilmaz, E. Kurt, and H. Kaya, "A Smart Home Security System with Face Recognition and Motion Detection," International Conference on Artificial Intelligence and IoT Security, 2022.
[22] Kumar and R. Sharma, "IoT-based Intrusion Detection System for Smart Homes," Journal of Emerging Technologies in Computing and Security, 2021.
[23] Wu, L. Feng, and X. Tang, "Cloud-Connected Home Security Systems with AI-based Anomaly Detection," Proceedings of the IEEE International Conference on Smart Computing, 2023.
[24] S. Anand and S. Ghosh, "A Real-time IoT-based Home Security Monitoring System," International Journal of Security and Surveillance Technologies (IJSST), 2022.