Patrolling System for Institution

Suvarna Aranjo, Thanga Selva, Pranjal Yadav, Tania Mondal
Department of Information Technology, Xavier Institute of Engineering Mahim, Mumbai India

Abstract—A transformative security paradigm, strengthened by Internet of Things (IoT) sensors, artificial intelligence (AI), and a vast dataset, has emerged because of the integration of cutting-edge technologies in an era characterized by increasing security challenges. This cutting-edge system is painstakingly built to detect trespassers and undesired activity as well as to handle data from a variety of sensors in an intelligent manner. By integrating facial recognition software, temperature sensors, and other sensors, the patrolling robot is transformed into an intelligent sentinel with advanced threat detection capabilities. A vast dataset combined with AI algorithms enables the system to change and grow, moving from reactive to proactive security measures. Response times are improved overall because real-time communication capabilities guarantee the timely delivery of important information to the appropriate persons. With its versatility, accuracy, and instantaneous response, this abstract offers an overview of the multidimensional strategy of a patrolling robot that makes use of IoT and AI technologies, revolutionizing the field of institutional security.

Keywords: Automation, Emergency Protocols, Audits, Adaptability, Technology Integration, Surveillance, Patrolling System, and Mobile Applications.

1. INTRODUCTION

The introduction of cutting-edge technologies has led to a revolutionary approach in the constantly changing field of security and surveillance: the use of sophisticated patrolling robots equipped with artificial intelligence (AI), a large dataset, and an advanced array of Internet of Things (IoT) sensors. The goal of this in-depth investigation is to analyze the nuances of a cutting-edge security framework that has been painstakingly created to apprehend trespassers and identify undesired activity in a dynamic institutional setting. The integration of GPS technology, temperature sensors, ultrasonic sensors, and facial recognition software results in an intelligent sentinel that can recognize security threats and adjust to its environment. The integration of IoT sensors, which creates a network connectedness where real-time data from several sources converges to generate a comprehensive and adaptive threat analysis, is the fundamental component of this sophisticated patrolling system. By adding a layer of environmental awareness through the deployment of temperature and ultrasonic sensors, the patrolling robot's response to possible security breaches is improved as it can identify abnormalities in the surrounding environment. When GPS is added, the patrolling robot becomes a geographically aware machine. This makes it possible to navigate predetermined routes precisely, guaranteeing effective coverage of the institution's grounds. Furthermore, GPS makes it easier to record locations accurately, which improves the responsible personnel's situational awareness and makes the reaction mechanism more efficient.

2. OBJECTIVE

1. To collect a range of environmental data, implement and integrate several IoT sensors, such as GPS modules, temperature sensors, and ultrasonic sensor guidelines.
2. Create and deploy advanced AI systems that can scan IoT sensor data, recognize trends, and make wise judgments for security reactions and intrusion detection.
3. Create a comprehensive dataset that includes a range of environmental circumstances, patterns for facial recognition, and events that could pose a threat. Make use of this dataset to train and iteratively refine the AI algorithms for increased precision.
4. By using temperature sensors to detect environmental abnormalities, you may empower the patrolling robot to recognize unlawful activity or intruders based on variations in usual temperature trends.
5. Use ultrasonic sensors to detect and avoid obstructions so the robot can navigate on its own without inadvertently running into items or barriers.
6. Include face recognition technology in the system to recognize people and discriminate

between authorized.

7. employees as well as any dangers. This guarantees targeted reactions and strengthens security safeguards.
8. Use GPS technology to provide accurate mapping and navigation so that the patrolling robot can find and follow designated routes and areas of interest.
9. Install a real-time communication module so that when the patrolling robot notices strange activity or intruders, it can immediately send information to the appropriate staff or a central control system.
10. Reduce the requirement for continual human intervention by designing the patrolling robot for autonomous operation. The robot's autonomy enables it to function well in a variety of settings and circumstances.

3. PROPOSED SYSTEM

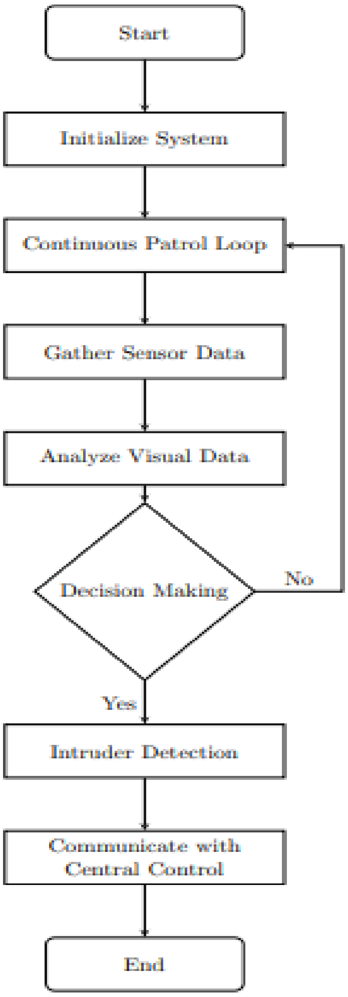

Figure 1: Flow Chart

Our suggested system has a flowchart that we have created. The main actions and elements involved in the functioning of a patrolling robot with sensors, cameras, and communication capabilities are depicted in the simplified flowchart below. The primary phases of the patrolling robot's functioning are depicted in this flowchart, including initialization, the continuous patrol loop, intruder detection, and communication with a remote operator or central control system. Of course! Let's dissect the patrolling robot's flowchart:

1. Initialize System:

The initialization of the system involves configuring cameras, configuring sensors (such as temperature, ultrasonic, and infrared), and setting up communication protocols (Wi-Fi, Bluetooth).

2. Patrol Loop:

A continuous patrol loop with the robot following a predetermined route forms the basis of the system. In this cycle, the robot carries out several tasks: - Collect Sensor Data, Examine Visual Data, and Make Decisions.

3. Intruder Detection:

Throughout the patrol loop, the flowchart listens for any unusual sounds. An intruder detection sequence is triggered when a sound anomaly is found, which results in an alarm and a predetermined action. The patrol cycle is repeated if no anomalies are found.

4. Communication:

The robot may receive remote commands or send data to a central control system. This communication feature makes sure the robot can exchange data it has collected, maintain its status, and receive commands or feedback.

5. End:

The flowchart ends, indicating that the system is no longer in operation.

To sum up, the flowchart depicts the high-level procedures that a patrolling robot goes through while navigating its surroundings, gathering sensor data, analyzing visual cues, making judgments, spotting intruders, and updating a central control system or remote operators on its status. The robot is constantly keeping an eye on its surroundings and reacting to any threats or environmental changes thanks to the continuous.

4. HARDWARE AND SOFTWARE REQUIREMENTS

A. Hardware Requirements:

1. IR SENSOR:

In this project, a robot is programmed to move automatically along a predetermined course using an infrared sensor. The infrared sensor is positioned ahead and to the sides of the robot to identify potential impediments. For the robot to follow predetermined paths and lines on the floor, we are additionally mounting one IR sensor on its underside. The sensors monitor the amount of time it takes for the infrared light to reflect after emitting it. The robot can change its course to prevent collisions if it detects an obstruction, enabling safe and easy navigation.

2. Sound sensor:

This robot has a sound sensor installed so that it can dynamically modify its patrol route in response to the sounds it detects. For example, it might reroute to investigate a loud noise or give priority to locations where activities are still going on. As a component of a larger security system, the sound sensor enables the robot to conduct frequent inspections and react to irregularities like sudden noises while on patrol.

3. Camera:

A patrolling robot's capabilities can be greatly increased by adding a camera, which gives it visual information about its surroundings. The patrolling robot's cameras allow it to visually monitor its surroundings and record video or take pictures in real-time. Analyses and monitoring can be performed using this visual data.

4. Raspberry Pi:

The robot's central processing unit is the Raspberry Pi. It can manage sensor data, execute the primary control algorithms, and coordinate the motions and actions of the robot. It can communicate with a range of sensors because of its GPIO pins. To collect information about the robot's surroundings, connect sensors including sound, infrared, camera, and ultrasonic sensors.

5. RESULT AND TEST CASES

Defining test cases and expected outcomes for a face-recognition patrolling robot for an institution entail modelling possible situations that the robot may run across. Here are a few sample test cases with the anticipated outcomes:

1. Test Case 1: Normal Patrol

Scenario:

The patrolling robot is navigating its predefined path within the institution, and no anomalies are detected.

Expected Results:

The robot finishes its patrol loop having found no anomalies or intrusions.

There are no security concerns during the regular patrol, according to the communication with the central control system.

2. Test Case 2: Intruder Detected

Scenario:

When a person is identified by the robot as not having the required authority, an intrusion detection scenario is initiated.

Expected Results:

The robot uses face recognition to identify the intruder.

The process of making decisions results in a modification of the patrol route.

Security staff are notified of the discovered intruder via communication with the central control system.

3. Test Case 3: Obstacle Detected

Scenario:

During the patrol, the robot runs across anything in its path.

Expected Results:

The robot uses its sensors to identify the obstruction.

The patrol route is modified because of the decision-making process to avoid obstruction.

An obstruction has caused the patrol path to shift, according to the communication with the central control system.

4. Test Case 4: Temperature Anomaly

Scenario:

The temperature sensor on the robot identifies an unusual rise in temperature in a particular area.

Expected Results:

The temperature anomaly is detected by the robot.

Investigating the reason for the anomaly or alerting the appropriate individuals may be steps in the decision-making process.

Details regarding the temperature anomaly are provided by the communication with the central control system.

5. Test Case 5: Communication Failure

Scenario:

There is a brief communication breakdown between the robot and the central control system.

Expected Results:

The robot keeps patrolling the area.

When there is no communication, the robot records the event and carries out its preprogrammed duties.

After the problem is fixed, the robot updates the central control system and communication is resumed.

6. Test Case 6: Battery Low
Scenario:
During the patrol, the robot's battery level falls below a certain threshold.
Expected Results:
The low battery level is detected by the robot.
Deciding entails either going back to a charging station or alerting staff to replace the battery.
The communication with the central control system indicates the low battery status.

These test cases encompass a range of scenarios that could be encountered by a patrolling robot, such as regular operations, security breaches, anomalies in the environment, and problems with the system. To make sure the robot acts as planned and reacts to various circumstances, testing is essential. It's crucial to remember that to verify the robot's performance in a variety of environments, real-world simulations and hardware integration would be required during actual testing.

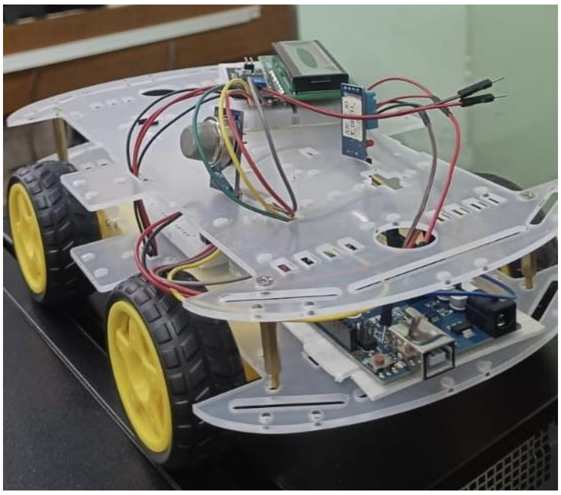

Figure 2: Patrolling Robot

6. CONCLUSION AND FUTURE WORK

The purpose of establishing this patrolling robot is that to keep the college campus secure. The camera will send a signal to the Raspberry Pi model when a human - being is in the ambient of the Robot. In turn, the camera module immediately captures an image and sends it to the web page. The robot will detect sounds as well in its surroundings with the help of sound sensors. It captures and sends the images directly to the control monitor room, for further actions. The robot can be used for a variety of purposes, such as fire alarm, burglar alarm, and temperature monitoring. Humans will be replaced by robots in some jobs and complemented by them in many others. Robotics has the potential to positively transform lives and work practices, raise efficiency and safety levels and provide enhanced levels of service. Robotics technology influences every aspect of work security. Robots are going to be a part of our society in the future. The robots may be for good and bad they will help us in doing things we can't do Robots are likely going to help us in securing our surroundings. At present security-related roles can see significant risk to workers reduced by implementing robotic guards in their place.

7. REFERENCES

[1] Ghanem Osman Elhaj Abdalla, T. Veeramanikandasamy “Implementation of Spy Robot for A Surveillance System using Internet Protocol of Raspberry Pi” May 19-20, 2017, India.
[2] Takato Saito and Yoji Kuroda “Mobile Robot Localization by GPS and Sequential Appearance-based Place Recognition” Japan, December 15-17.
[3] Alexander Lopez, Renato Paredes, Diego Quiroz, Gabriele Trovato and Francisco Cuellar “Robotman: A Security Robot for Human-Robot Interaction” Hong Kong, China, July 2017.
[4] By Stefan Witwicki, José Carlos Castillo, Joao Messias, Jesús Capitán, Francisco S. Melo, Pedro U. Lima, and Manuela Veloso “Autonomous surveillance Robots” 4 August 2017.
[5] Tahzib Mashrik, Hasib Zunair, Maofic Farhan Karin “Design and Implementation of Security Patrol Robot using Android Application” 2017 IEEE.
[6] N. Vishwanath, S Perumal Sankar “Multisensor Smart Robot for Border Security Surveillance with Human Action Prediction” August 2019.
[7] Meshram Priyadarshani Rajkumar, Prof. Mrs. S. P. Tondare and Prof. Dr. Mrs. S. P. Gaikwad “Design and Realization of Automatc Video-Based Docking Structure For Home Surveillance Robots By Using Raspberry Pi.” 11, November 2017.3
[8] Priyanka Bhor, Pooja Vashiwale, Prof. Vijay.N.Patil, “Surveillance of Background Activities using MOG, ViBe and PBAS”, International Journal for Research in Engineering Application & Management (IJREAM) ISSN : 2454-9150 Vol-03, Issue 01, Apr 2017.