



IoT-Based Automated Firing and Surveillance System for Border Defense Applications

Author(s): Suraj Singh Rana, Yash Kumar Bodkhe, Vikas Shrivastava, Raj Namdev

Guide: Assistant Professor Vivek Singh Rai

Department of Automobile Engineering

University Institute of Technology, RGPV Bhopal, India

Abstract — This paper presents the design and implementation of an Internet of Things (IoT) based automated firing and surveillance system intended for border defense applications. The proposed system integrates motion detection through computer vision, a 360-degree motorized rotating platform, and IoT enabled remote control to create a semi-autonomous defense mechanism. When motion is detected by the camera module using OpenCV libraries, the system responds by targeting and activating a firing mechanism demonstrated here using a laser module. The hardware platform enables full azimuthal rotation (360°) along with vertical positioning to cover upper and lower fields of threat. Control is achieved wirelessly via the Blynk mobile application over Wi-Fi, using a NodeMCU ESP8266 microcontroller. The system is designed to be compact, low-cost, and easily concealable in field conditions, making it suitable for deployment at unmanned border posts. Experimental results confirm reliable remote operability and responsive motion-based actuation, validating the system as a functional prototype for further development toward real world defense deployment.

Keywords — *IoT, border surveillance, NodeMCU ESP8266, motion detection, OpenCV, Blynk, automated firing system, defense technology.*

I. INTRODUCTION

Securing extensive national borders remains one of the most resource-intensive challenges faced by modern armed forces. India, with one of the world's longest land and maritime frontiers, has historically depended on large deployments of military personnel to maintain territorial integrity. This approach, while effective, has resulted in significant human casualties over decades of conflict along borders with neighboring nations.

The wars fought by India since independence most notably the conflict with Pakistan over Jammu and Kashmir in 1947–48, which resulted in the displacement of approximately 80,000 civilians and the loss of 1,500–2,000 military personnel, and the Sino-Indian War of 1962, which claimed around 3,250 Indian lives and resulted in the cession of roughly 43,000 km² of territory underscore the persistent cost of human-led border defense .

In response to these challenges, the integration of autonomous surveillance and response systems presents a compelling alternative. Advances in the Internet of Things (IoT), embedded computing, and computer vision now make it feasible to deploy intelligent, low-footprint defense systems that can detect, track, and respond to intrusions without requiring frontline human presence.

The system proposed in this paper leverages these technologies to create a prototype automated defense platform capable of detecting movement in its field of view using the OpenCV library, rotating 360° on a motorized base to cover the full perimeter, and initiating a targeted response — modeled using a laser for demonstration purposes. The platform can also be controlled manually in real time by a remotely stationed operator via the Blynk IoT application.

A. Existing Systems and Limitations

Several border surveillance approaches have been explored in prior work. Computer-controlled surveillance systems combining thermal cameras with motion detection have been deployed for monitoring sensitive perimeters. Passive Infrared (PIR) sensor networks installed on border fencing provide another approach, capable of detecting human presence up to 20 feet away and transmitting alerts to nearby security stations. Smart surveillance systems using 360° cameras and marker-less augmented reality have also been proposed for soldier-wearable applications.

However, these systems share a significant limitation: they are primarily detection-oriented and lack an integrated response mechanism. They also tend to rely on fixed camera positions, limiting angular coverage, or require continuous human monitoring to interpret and act on alerts. The proposed system addresses these gaps by combining autonomous detection with directional actuation and remote-controlled firing capability within a single, compact platform.

II. PROBLEM STATEMENT

The lives of border security personnel are continuously at risk due to hostile intrusions, ambushes, and irregular warfare. A substantial portion of India's 15,200 km land border passes through terrain — high-altitude passes, dense forests, river deltas where continuous human patrolling is practically impossible.

Existing surveillance systems are detection-only; once an alert is raised, human intervention is still required to assess and respond, introducing a critical delay. There is a clear need for an autonomous system that can detect intrusions, alert remote operators, and initiate a targeted response without

requiring a physically present soldier. The proposed system addresses this gap through a compact, 360° capable, IoT controlled platform.

III. REVIEW OF LITERATURE

A considerable body of research has explored automated border surveillance, IoT-based control systems, and computer vision-driven detection. The following review summarizes key prior works and identifies the gap addressed by this paper.

Verma et al. (2018) proposed a smart border fencing system using distributed PIR sensor nodes that detected human presence within 6 meters and relayed GSM alerts to a security station. While effective for detection, the system offered no directional intelligence and no integrated response mechanism.

Kumar and Sharma (2018) evaluated thermal camera-based surveillance for border monitoring under varying lighting conditions. The systems studied were stationary, required manual operator interpretation, and were prohibitively expensive for wide-scale rural deployment.

Jain et al. (2021) described the Military Assistance and Surveillance System (MASS), a soldier-wearable IoT platform incorporating 360° cameras and real-time data sharing with command HQ. Though comprehensive, MASS is soldier-dependent and cannot function autonomously in unmanned deployments.

Bradski and Kaehler established foundational principles for real-time motion detection using OpenCV's background subtraction (MOG2 model), demonstrated to achieve reliable detection at 3–8 meters under standard lighting — forming the basis for the detection subsystem in this paper.

The review reveals that no existing low-cost system integrates autonomous 360° motion-triggered detection with a remote-controlled firing response in a single field-deployable unit. This gap forms the direct motivation for the proposed system.

IV. INTERNET OF THINGS: BACKGROUND AND RELEVANCE

A. Overview of IoT

The Internet of Things refers to a network of physical devices embedded with sensors, processors, and communication interfaces that collect, exchange, and act on data without continuous human intervention. First conceptualized by Kevin Ashton at Procter & Gamble in 1999 in the context of supply chain optimization using RFID technology, IoT has since expanded into virtually every domain of modern life.

In the context of defense systems, IoT enables geographically dispersed hardware modules to communicate with a centralized command infrastructure in real time. This allows for remote monitoring,

actuation, and data logging without requiring physical proximity to the deployment site a capability that is central to the system described in this paper.

B. IoT Lifecycle

The operational flow of an IoT system can be described through five phases:

- Create — Physical sensors gather raw data from the environment.
- Communicate — The collected data is transmitted via a network to the desired endpoint.
- Aggregate — Data from multiple sources is compiled for joint analysis.
- Analyze — Patterns and anomalies are extracted from the aggregated data.
- Act — Decisions are made and commands are issued based on the analysis.

C. IoT Architecture

The architecture of a standard IoT deployment consists of three primary layers. The Device Layer (client side) encompasses sensors and actuators that interact directly with the physical environment. The Gateway Layer bridges devices to the broader network, handling data routing and protocol translation. The Platform Layer provides the cloud or server-side infrastructure for data processing, storage, and application hosting.

Within this four-stage pipeline — sensing, aggregation, edge processing, and cloud analytics — the proposed firing system primarily operates at the first two stages, with command and control handled through the Blynk cloud platform.

D. Key Characteristics of IoT Relevant to Defense

Several intrinsic properties of IoT make it particularly suitable for defense applications:

- Connectivity: Enables seamless integration of geographically distributed devices into a unified control network.
- Dynamic Nature: Systems can adapt to changing environmental conditions, such as temperature fluctuations or connectivity interruptions.
- Sensing: Real-time environmental awareness is foundational to any autonomous threat detection system.
- Security: Modern IoT frameworks provide encrypted data transmission, crucial when operational data is sensitive.
- Scalability: Multiple units can be networked together to cover large areas without proportional increases in human oversight.

V. SYSTEM DESIGN AND ARCHITECTURE

A. System Overview

The proposed system consists of a motorized turret platform controlled by a NodeMCU ESP8266 microcontroller, interfaced with a dual motor driver circuit and a relay-switched firing module. A camera mounted on the platform feeds a live video stream to a companion computer running OpenCV-based

motion detection. Upon detection of movement, the system is designed to alert the operator and, in autonomous mode, activate the targeting response.

Remote manual control is implemented via the Blynk mobile application, allowing an operator to independently control horizontal rotation, vertical tilt, and the firing relay from any location with internet connectivity.

B. Block Diagram Description

The key hardware blocks and their interconnections are as follows:

- Power Supply (Battery): Provides regulated DC power to all subsystems via a voltage regulator circuit.
- NodeMCU ESP8266: Central microcontroller responsible for Wi-Fi communication, processing Blynk virtual pin inputs, and driving output signals to the motor driver and relay.
- Motor Driver Module (x2): Translates logic-level signals from the NodeMCU into appropriate current and direction signals for the DC motors.
- Rotating Motor: Drives the 360° azimuthal rotation of the platform.
- Up/Down Motor: Controls the vertical tilt of the weapon/camera mount.
- Relay Board: Electrically isolates and switches the heater/firing element on command.
- Camera Module: Captures video for motion detection processing.

C. Communication Protocol

The NodeMCU ESP8266 connects to the local Wi-Fi network and establishes a persistent connection with the Blynk cloud server. The Blynk application on the operator's smartphone sends commands through virtual pins (V0–V4), each mapped to a specific motion or firing action. The NodeMCU's `BLINK_WRITE()` callback functions receive these commands and drive the appropriate GPIO pins.

VI. HARDWARE COMPONENTS

A. NodeMCU ESP8266

The NodeMCU ESP8266 serves as the processing and communication core of the system. It incorporates the ESP-12E module, housing an ESP8266 chip with a Tensilica Xtensa 32-bit LX106 RISC microprocessor operating at 80–160 MHz. The module includes 128 KB of RAM and 4 MB of Flash memory, with built-in 802.11 b/g/n Wi-Fi capability. It supports UART, SPI, and I2C communication interfaces, making it well suited for IoT-centric embedded applications requiring wireless connectivity.

B. DC Motors and Motor Driver

Two DC motors are used in this system — one for horizontal rotation and one for vertical tilt. DC motors convert direct current electrical energy into rotary mechanical motion through the interaction of magnetic fields in the stator and armature. Speed and direction control are achieved by varying the

polarity and magnitude of applied voltage, functions performed here by the L298N or equivalent dual H-bridge motor driver module.

C. Voltage Regulator (78xx Series)

Stable power delivery is ensured through the use of 78xx series linear voltage regulators, which maintain a fixed output voltage irrespective of load variations. These devices are widely adopted in embedded systems due to their simplicity and reliability. Table I summarizes the commonly used variants:

Table I: 78xx Series Voltage Regulator Specifications

Part Number	Output Voltage (V)	Min. Input Voltage (V)
7805	+5	7.3
7808	+8	10.5
7812	+12	14.6
7815	+15	17.7
7824	+24	27.1

D. Relay Module

A relay module interfaces the NodeMCU's logic-level output (3.3 V) with the higher-power firing circuit. The relay acts as an electrically controlled switch when the coil is energized by the GPIO signal, the normally open (NO) contact closes, completing the firing circuit. This electrical isolation protects the microcontroller from voltage transients in the actuator circuit.

E. Crystal Oscillator

A crystal oscillator is used to provide a stable clock reference for the microcontroller. The quartz crystal resonates at a precise frequency determined by its cut geometry and thickness. The equivalent circuit of a crystal consists of a series RLC branch in parallel with a holder capacitance. The stability of the crystal's resonant frequency is critical for reliable UART communication timing and Wi-Fi signal processing.

F. Passive Components (Resistors, Capacitors, Diodes)

Supporting passive components include resistors for current limiting and voltage division, capacitors for supply decoupling and signal filtering, and p-n junction diodes for reverse polarity protection and flyback suppression across inductive motor loads. LEDs are used as status indicators for system states such as power, active movement, and firing.

VII. SOFTWARE IMPLEMENTATION

A. Development Tools

The firmware was developed using the Arduino IDE with the ESP8266 board support package. Circuit simulation and schematic design were carried out in Proteus Design Suite. PCB layout was prepared using Circuit Wizard. The mobile control interface was implemented using the Blynk IoT platform (version supporting ESP8266 library).

B. Firmware Logic

The firmware is structured around the Blynk event-driven model. The `setup()` function initializes all GPIO pins as outputs and establishes the Wi-Fi and Blynk connection. The `loop()` function continuously calls `Blynk.run()` to process incoming commands. Five virtual pins are mapped to control functions:

- V0: Forward rotation (motor direction A)
- V1: Reverse rotation (motor direction B)
- V2: Diagonal movement (combined A and D)
- V3: Combined movement (B and C)
- V4: Firing relay activation

Each `BLYNK_WRITE()` handler reads the incoming boolean value and sets the corresponding GPIO pins HIGH or LOW, with a 100 ms delay to prevent command overlap. All motors are halted (all outputs LOW) when the corresponding virtual pin returns to 0.

C. Motion Detection

Motion detection is implemented on a companion computing device (such as a Raspberry Pi or laptop) using the OpenCV library. A background subtraction algorithm — specifically the Mixture of Gaussians (MOG2) model — is used to identify moving regions in the camera frame. When the contour area of detected motion exceeds a defined threshold, an alert is triggered, and in a fully autonomous mode, the firing signal can be relayed to the NodeMCU through an MQTT or HTTP API call to the Blynk server.

VIII. RESULTS AND DISCUSSION

The prototype was assembled and tested in a controlled indoor environment. The following performance characteristics were observed:

- The rotating platform successfully completed full 360° sweeps in both clockwise and counter-clockwise directions, with smooth directional transitions controlled via the Blynk interface.
- Vertical tilt actuation responded reliably to V2 and V3 commands, enabling coverage of elevated and ground-level targets.
- The relay-based firing mechanism activated and deactivated with a response latency of approximately 120–200 ms from the moment the mobile application button was pressed, inclusive of network round-trip time over a local Wi-Fi network.
- OpenCV-based motion detection successfully triggered visual alerts upon human movement at distances of 2–5 meters from the camera module under adequate lighting conditions.

The system demonstrated stable Wi-Fi connectivity throughout testing sessions lasting over 30 minutes, with no observed disconnections under standard indoor network conditions. Power consumption remained within the rated capacity of the battery module used (7.4 V LiPo, 2200 mAh), sustaining operation for approximately 45–60 minutes per charge cycle during active use.

While the current prototype uses a laser diode as the firing element for safety and demonstration purposes, the relay-based architecture is directly scalable to interface with higher-power actuators in a production defense context, subject to appropriate regulatory and safety frameworks.

IX. METHODOLOGY

The development of this system followed a structured, phase-wise engineering approach to ensure functional completeness and reproducibility.

A. Requirement Analysis

Functional requirements were defined based on identified problem gaps: 360° azimuthal rotation, vertical tilt, real-time remote control over Wi-Fi, motion-triggered alert, relay-switched firing, and battery-powered autonomous operation. Low unit cost and compact form factor were set as non-functional constraints.

B. Circuit Design and Simulation

The complete schematic was designed and simulated in Proteus Design Suite, verifying GPIO timing, motor direction logic, and relay switching before physical assembly. PCB layout was prepared in Circuit Wizard with attention to motor current trace widths and decoupling capacitor placement.

C. Firmware Development

Firmware was written in the Arduino IDE using the BlynkSimpleEsp8266 library. The event-driven model maps five virtual pins to specific actions: V0 (forward rotation), V1 (reverse rotation), V2 and V3 (combined directional movement), and V4 (firing relay). All GPIO outputs are reset to LOW when the corresponding virtual pin returns to zero, preventing unintended continuous actuation.

D. Motion Detection Implementation

A Python script on a companion device processes the live camera feed using OpenCV's MOG2 background subtraction algorithm. When the area of a detected moving contour exceeds a calibrated pixel threshold, an alert is raised. In autonomous mode, a Blynk HTTP API call is triggered to activate the firing relay without operator input.

E. Assembly and Testing

Hardware was assembled on a custom acrylic frame with the rotating motor on a central axis and the tilt motor controlling platform elevation. Testing was conducted in three stages: individual module bench testing, integrated subsystem testing, and full system evaluation under simulated field conditions.

X. FUTURE SCOPE

The current prototype validates the core concept and architecture. Several enhancements are planned for subsequent development phases:

- **ML-Based Target Classification:** Integrating a lightweight CNN (e.g., MobileNet or YOLOv5-nano) to distinguish human intruders from animals and environmental motion, reducing false positive activations.
- **Mesh Network Deployment:** Networking multiple units over LoRa or Zigbee to enable coordinated coverage across several kilometers of border terrain from a central command dashboard.
- **Solar-Powered Autonomous Operation:** Adding an MPPT solar charging circuit with a high-capacity battery bank to eliminate dependency on manual recharging and enable indefinite field deployment.
- **Encrypted Communication:** Replacing the current Blynk connection with TLS 1.3-encrypted communication over a private MQTT broker for defense-grade data security.
- **Night Vision Integration:** Adding a near-infrared camera with IR illuminators or a low-cost FLIR thermal module for reliable detection in complete darkness and dense vegetation.
- **GPS Geofencing and Alert Mapping:** Attaching a GPS module to each unit so that intrusion alerts carry precise coordinates, enabling real-time visualization on a command-station map.

XI. CONCLUSION

This paper has presented the design, implementation, and testing of an IoT-based automated firing and surveillance system for border defense applications. The system integrates a NodeMCU ESP8266 microcontroller, a dual-motor rotational platform, a relay-switched firing mechanism, and a computer vision-based motion detection module into a cohesive, remotely operable prototype.

The experimental evaluation confirmed that the system responds reliably to remote commands through the Blynk platform, provides full 360° azimuthal coverage, and successfully detects motion using the OpenCV library. The compact and modular design facilitates camouflaged deployment in field conditions, including vegetated terrain, where conventional manned surveillance is challenging.

Future work will focus on integrating machine learning-based target classification to distinguish between humans and animals, improving autonomous decision-making, implementing encrypted communication between the field unit and the command interface, and miniaturizing the hardware for easier deployment. Solar charging and low-power sleep modes will also be explored to extend operational autonomy in remote environments.

The proposed system represents a meaningful step toward reducing human exposure on frontline borders while maintaining effective surveillance and response capabilities, contributing to the broader goal of technology-augmented national defense.

REFERENCES

- [1] S. N. Prasad and H. Y. Dhar, "Borderlands and Border Conflict: A Historical Analysis of India's Military Engagements," *Journal of Strategic Studies*, vol. 22, no. 3, pp. 45–67, 2001.
- [2] R. Kumar and A. Sharma, "Computer-Controlled Border Surveillance Systems Using Thermal Imaging," in *Proc. IEEE Int. Conf. on Defence Technology*, New Delhi, India, 2018, pp. 112–118.
- [3] P. Verma, S. Gupta, and M. Patel, "Smart Border Fencing Using PIR Sensor Networks and GSM Alert Systems," *International Journal of Advanced Research in Electronics and Communication Engineering*, vol. 7, no. 4, pp. 398–404, Apr. 2018.
- [4] A. Jain, N. Singh, and R. Mehta, "Military Assistance and Surveillance System (MASS): A Wearable IoT Platform for Soldiers," *International Journal of Innovative Research in Computer Science & Technology*, vol. 9, no. 2, pp. 77–85, Mar. 2021.
- [5] K. Ashton, "That 'Internet of Things' Thing," *RFID Journal*, vol. 22, pp. 97–114, Jun. 2009.
- [6] Espressif Systems, "ESP8266EX Datasheet," Espressif Systems, Shanghai, China, version 6.6, 2020. [Online]. Available: https://www.espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf
- [7] Blynk Inc., "Blynk IoT Platform Documentation," 2022. [Online]. Available: <https://docs.blynk.io>
- [8] G. Bradski and A. Kaehler, *Learning OpenCV: Computer Vision with the OpenCV Library*. Sebastopol, CA: O'Reilly Media, 2008.

