IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 11 ISSUE : 01 Print / Issue Publication Date: May 2026

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2026.v11i01.003

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 01, ISSN No. 2455-2143, Pages 14-19
Published Online May 2026 in IJEAST (http://www.ijeast.com)

IOT-BASED UNMANNED GROUND VEHICLE FOR ARMY SURVEILLANCE

Deepak P, Vishwa S, Vishaal S
Department of Computer Science and Engineering
SRM Valliammai Engineering College
Chennai, India

Abstract: **Military reconnaissance in unmapped or hostile border regions exposes personnel to severe risks, such as enemy fire and hidden explosive devices. While autonomous defense platforms aim to reduce human casualties, existing robotic systems frequently suffer from high power consumption and rely heavily on fragile communication networks (like Wi-Fi or cellular data) that are easily jammed or absent in remote areas. To overcome these vulnerabilities, this paper presents a highly optimized, low-power Internet of Things (IoT)-based Unmanned Ground Vehicle (UGV) tailored for military surveillance.**

The proposed architecture shifts the computational load from power-heavy microcomputers to an efficient ESP32 microcontroller. It establishes resilient, off-grid telemetry using a Long Range (LoRa) sub-GHz transceiver, enabling secure data transmission over several kilometers despite physical obstacles or electronic interference. To operate effectively in zero-visibility environments (e.g., fog, smoke, or total darkness), the UGV utilizes a dual-vision system that prioritizes an MLX90640 thermal infrared array for detecting human heat signatures, significantly conserving bandwidth and power compared to continuous video streaming. Furthermore, the vehicle integrates ultrasonic obstacle avoidance, GPS tracking, and an IMU-based anti-tamper mechanism that instantly alerts operators to physical breaches without the risk of catastrophic false positives. Projections show this design reduces current draw by up to 60%, allowing for continuous surveillance deployments exceeding 12 hours while providing commanders with reliable, real-time tactical data.

Keywords: **Unmanned Ground Vehicle (UGV), Military Surveillance, Internet of Things (IoT), LoRa Communication, Thermal Imaging Detection, Sensor Fusion, Low-Power Architecture, Anti-Tamper Security.**

I. INTRODUCTION

Doing military reconnaissance is really dangerous work. When soldiers have to patrol border areas that aren't mapped well, they run into big risks like hostile fire or hidden bombs (IEDs). Most modern defense plans try to lower these human risks, which fits right in with UN goals for health and peace. The problem is that seeing targets in these places is tough. Basic cameras don't work well when there's fog, smoke, or when it's dark out. We really need automated systems that can map areas and find people no matter what the weather looks like. Because of this, we built an IoT-based Unmanned Ground Vehicle (UGV) to handle these risky patrol jobs.

There are already some robotic platforms out there, but they usually depend on 4G, 5G, or Wi-Fi. Out in remote border spots, those networks are basically useless since they either aren't there or get jammed easily. Our setup uses a Long Range (LoRa) radio transceiver instead. This lets us have an off-grid communication system that sends sensor data over a few kilometers while using almost no battery power. It also makes it a lot harder for someone to jam the signal using standard equipment.

Physical security is another big headache. If these robots are left in isolated spots, they could be captured or messed with. Most systems just show the signal dropped without saying why it happened. We fixed this by adding an anti-tamper setup based on motion. By tracking how the robot is tilted and how fast it's moving, it can tell if it's just driving over bumps or if someone actually picked it up. If someone tampers with it, the UGV sends an encrypted alert to the hub right away. Then, the operators can start defensive steps immediately.

Basically, this project provides a secure way to do remote surveillance without using much power. By putting together thermal imaging to find people, ultrasonic sensors for driving, GPS for locations, and LoRa for talking to the base, the UGV works as a solid scout unit. It gives commanders real-time info they can actually use to better protect the perimeter and keep people out of danger.

II. LITERATURE REVIEW

Over the last decade, plenty of research has looked into adding autonomous systems and sensors to military operations. While recent work has made strides with microcontrollers and Unmanned Ground Vehicles (UGVs), there are still major hurdles to overcome.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 01, ISSN No. 2455-2143, Pages 14-19
Published Online May 2026 in IJEAST (http://www.ijeast.com)

For instance, Mandalik et al. built a solid foundation using the STM32 microcontroller for multi-sensor UGVs. The problem? Relying purely on the STM32 and high-draw parts eats up power fast, making it impossible to keep the vehicle out in the field for prolonged deployments. To handle visibility issues, Patel and Chen used edge Artificial Intelligence (AI) to spot human heat signatures. While highly accurate, edge AI requires robust processors that run hot and drain batteries heavily. Plus, their setup easily gets confused by burning debris or warm vehicle engines—things you see everywhere in combat zones.

Rodriguez and Yamamoto tried a different angle, managing cameras, ultrasonic, and thermal sensors with Raspberry Pi microcomputers. However, using a Raspberry Pi proved to be a critical flaw. It overheated and throttled during long thermal imaging sessions, making it much too fragile for extreme military environments like deserts or high altitudes.

Physical security is another major vulnerability. Novak and Desai created an anti-capture system that uses accelerometers and gyroscopes to trigger an explosive self-destruct if the vehicle is lifted. In theory, it sounds great. In practice, rough terrain caused the sensors to drift, leading to

Vulnerability	**Description**
Operational Endurance	High-power sensors and microcomputers (e.g., Raspberry Pi) drain standard batteries rapidly, limiting mission length.
Communication Resilience	Heavy reliance on cellular or Wi-Fi signals leaves the vehicle highly susceptible to electronic warfare and jamming.
Environmental Limitations	Traditional visual cameras fail in low-light, fog, or smoke, while complex Edge AI thermal models overheat the processing unit.
Physical Security	Autonomous self-destruct mechanisms triggered by vibrations lead to critical false positives and loss of hardware

Table. 1. Existing system vulnerabilities

catastrophic false positives where the vehicle blew itself up. Lee and Gupta improved on this by linking accelerometer alerts to LoRa networks , but they still allowed the system to self-destruct without human confirmation—an unacceptable risk during active combat.

Across all these studies, there is a constant battle between data bandwidth and battery life. Heavy video feeds require cellular or Wi-Fi networks , which demand a lot of power and rely on fragile infrastructure. Switching to low-power networks like LoRa solves the power issue but lacks the bandwidth for video streaming. This leaves a huge gap in how to efficiently use thermal imaging in the field. Very few researchers have tried using a low-power microcontroller to scan a simple, low-resolution thermal grid and transmit only lightweight outcome alerts over LoRa. Lastly, navigating when GPS is actively jammed remains tough. Wang and Oliveira tried using inertial backups with LoRa mesh networking , but their system lost a lot of accuracy on rough terrain because mathematical errors quickly piled up in their dead-reckoning calculations.

III. PROPOSED SYSTEM ARCHITECTURE

To comprehensively mitigate the drawbacks identified in traditional scouting methods and existing robotic platforms, the proposed system employs a highly optimized, low-power, multi-sensor IoT architecture. The core philosophy of this design is to shift the computational burden away from power-hungry microcomputers and instead utilize efficient, task-specific microcontrollers coupled with long-range radio transmission. The central processing unit governing the entire mobile platform is the ESP32 microcontroller, selected specifically for its superior power-to-performance ratio, abundant General Purpose Input/Output (GPIO) pins, and native support for multiple communication protocols including Inter-Integrated Circuit (I2C) and Serial Peripheral Interface (SPI). wwws 2 details the specific operational ranges and limitations of the diverse sensor suite utilized within this architecture.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 01, ISSN No. 2455-2143, Pages 14-19
Published Online May 2026 in IJEAST (http://www.ijeast.com)

Sensor Module	Parameter	Operational Range
MLX90640 (Thermal)	Target Temperature	-40°C to 300°C
HC-SR04 (Ultrasonic)	Distance	2 cm to 400 cm
MPU6050 (IMU)	Accelerometer	±2g, ±4g, ±8g, ±16g
MPU6050 (IMU)	Gyroscope	±250, ±500, ±1000, ±2000 °/s
NEO-6M (GPS)	Positioning	Global (Outdoor Line-of-Sight
OV7670 (Camera)	Visual	Optical Line-of-Sight

Table.2.Sensor Module and their operations; specifications

A. Vision and Thermal Imaging Module

The surveillance capability of the UGV is driven by a sophisticated dual-vision approach, carefully designed to operate flawlessly regardless of environmental lighting or weather conditions. The system integrates a standard OV7670 optical camera module to provide live, daylight visual feedback to the remote operator. This visual stream is essential for basic terrain navigation and target identification during optimal conditions. However, the true tactical advantage is achieved through the secondary vision system: the MLX90640 thermal infrared sensor array.

Unlike standard night-vision cameras that require ambient light to amplify, the MLX90640 detects infrared radiation emitted by objects based on their inherent temperature. This thermal sensor features a 32x24 pixel array, providing a total of 768 individual temperature measurement points across its field of view. The sensor operates over the I2C bus and communicates directly with the ESP32. By continuously scanning these temperature points, the microcontroller can easily identify the distinct heat signatures of human bodies (typically radiating at approximately 37°C) against the cooler background of foliage, soil, or urban structures. This allows the UGV to detect enemy combatants hiding in total darkness, heavy rain, or behind thick artificial smoke screens deployed during tactical maneuvers.

B. Navigation and Tracking Module

To navigate safely across the unpredictable and highly uneven topographies typical of military deployments, the UGV is equipped with a robust autonomous obstacle detection network. This network relies on forward-facing HC-SR04 ultrasonic sensors. These sensors operate by emitting high-frequency sound waves and measuring the precise time it takes for the acoustic echo to return after reflecting off a physical barrier.

The ESP32 microcontroller processes these acoustic pings to calculate the distance d to an impending obstacle. The mathematical relationship is derived from the time of flight of the ultrasonic pulse, represented as:

$$d = \frac{v \times t}{2}$$

accidental crashes into rocks or walls without needing the operator to steer manually every second. At the same time, we handle location tracking using a NEO-6M GPS module. This module connects to multiple satellites to get the vehicle's exact coordinates, which are sent back to the base station continuously so we don't lose track of where the robots is during the mission

C. Long-Range Communication Module

The most important part of our design is using LoRa (Long Range) radio tech with the SX1278 transceiver. Most IoT projects just use Wi-Fi or 4G, but those need cell towers or routers to work. In a war zone, that infrastructure usually gets blown up or jammed by the enemy, making standard connections useless.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 01, ISSN No. 2455-2143, Pages 14-19
Published Online May 2026 in IJEAST (http://www.ijeast.com)

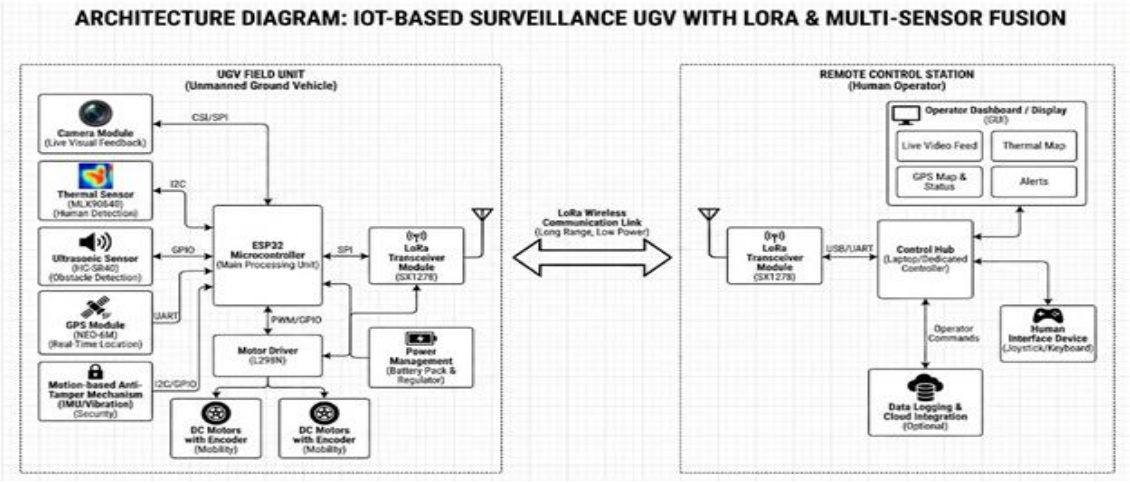

Fig. 1. Architecture diagram

The SX1278 works on sub-GHz ISM bands. It uses a special modulation called Chirp Spread Spectrum (CSS) which basically trades speed for crazy long range and signal strength. The ESP32 talks to the LoRa module over SPI. By tweaking the spreading factor and bandwidth, the UGV stays connected for several kilometers, even through thick trees or concrete walls where a normal Wi-Fi signal would just die.

D. **Security and Mobility Modules**

To keep the robot from being stolen, we built in a motion sensing system using the MPU6050 IMU. This chip has a 3-axis accelerometer and gyroscope to track how the UGV is tilted and moving. Usually, it just feels the normal vibrations of the wheels on the ground. But if someone tries to pick it up or if it gets flipped over by an explosion, the IMU sees a huge spike in acceleration. The ESP32 detects this pattern and immediately sends an anti-tamper alert over LoRa to tell the operator the hardware has been messed with.

The UGV moves using DC gear motors with encoders to keep track of distance. We control them with an L298N dual H-bridge driver that takes PWM signals from the ESP32 to set the speed. Everything runs on an 11.1V LiPo battery. Since the electronics are sensitive, we use a buck converter to step that power down to a steady 5V so nothing gets fried by voltage spikes.

IV. METHODOLOGY AND SOFTWARE ALGORITHMS

The way the UGV actually runs is focused on saving power. Instead of having the processor work at 100% all the time, the code uses an asynchronous polling loop. This stops the battery from draining too fast during long surveillance missions.

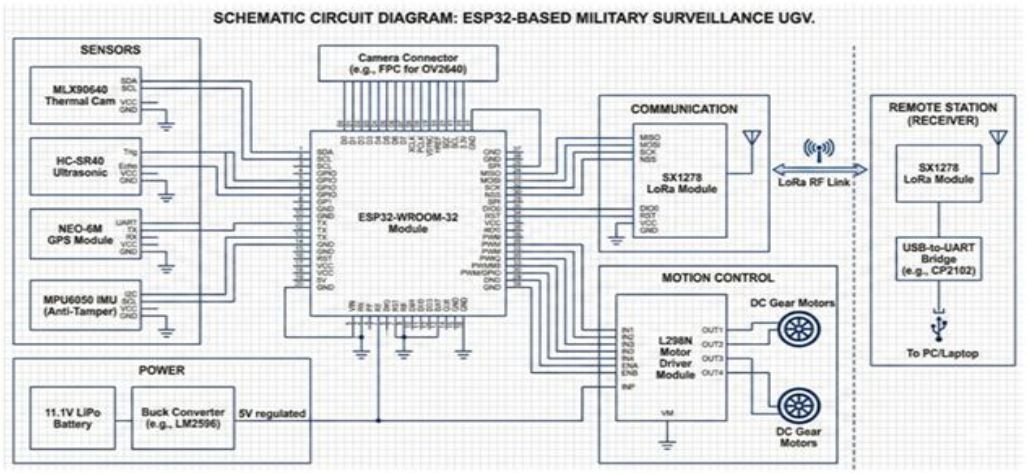

Fig. 2. Circuit Diagram

When you turn it on, the ESP32 goes through a setup phase to link with all the modules. It starts LoRa first to make sure it can talk to the remote station. We set the signal parameters to punch through obstacles as much as possible. After that, it calibrates the IMU, thermal, and GPS modules to get a good baseline for the current environment.

The main code uses a sensor fusion logic to find people. Streaming high-res video 24/7 uses way too much power and bandwidth, so we rely on the thermal array instead. The ESP32 scans the 768 points in the thermal matrix. If it finds a cluster of pixels that match human body heat, it triggers an alert. Only then does it wake up the optical camera to take a photo for confirmation, which saves a ton of energy.

The obstacle avoidance runs in the background. The ultrasonic sensors ping the area constantly, and if they see something too close, the code interrupts the motors. It tells the L298N driver to stop immediately and then runs a pathfinding routine where the robot turns to find a clear path before moving again. This keeps the UGV from getting stuck if there's any lag in the LoRa link

Meanwhile, the security code watches the data from the MPU6050. We use low-pass filters to ignore the vibrations from the motors and bumpy ground. If the acceleration change hits a certain threshold, the ESP32 stops normal data and broadcasts an encrypted distress signal over LoRa, so the base knows about the breach in less than a second.

On the user's end, the control station acts as the brain for the operator. It's just a second LoRa module hooked up to a laptop with a custom dashboard. This GUI takes the raw data and builds the thermal map, shows the GPS location on a tactical map, and pops up security alerts. The operator can use a keyboard or joystick to take over manually at any time, sending steering commands back through the secure LoRa link.

V. EXPECTED RESULTS AND DISCUSSION

Extensive component analysis suggests that the proposed ESP32-based architecture demonstrates improved operational endurance compared to traditional Raspberry Pi-based models. By utilizing a deep-sleep polling methodology and relying primarily on the MLX90640 thermal array rather than continuous visual streaming, the overall current draw of the system is projected to be reduced by up to 60%. Powered by an 11.1V, 5000mAh LiPo battery, the UGV is anticipated to achieve continuous surveillance deployments exceeding 12 hours, which is a significant extension over the 3 to 4-hour lifespan typical of high-compute existing systems.

The implementation of the SX1278 LoRa transceiver is expected to exhibit high communication resilience. In theoretical line-of-sight conditions, the telemetry link should remain stable at

distances up to 10 kilometers. In dense urban or forest environments, the 433MHz/868MHz sub-gigahertz frequency readily penetrates obstacles, maintaining a reliable connection at 2 to 3 kilometers. This capability addresses the communication breakdowns experienced by UGVs reliant on 2.4GHz Wi-Fi, which typically degrade within 200 meters of obstructed terrain.

Furthermore, the dual-vision multi-sensor fusion is anticipated to mitigate operational limitations imposed by environmental visibility. The thermal sensor will successfully identify human heat signatures in zero-visibility scenarios, operating independently of artificial smoke screens or pitch-black darkness that render the standard OV7670 camera ineffective. Finally, the IMU-based anti-tamper mechanism is calibrated to a highly specific lifting threshold, substantially reducing the false-positive self-destruct scenarios noted in previous literature while ensuring that unauthorized handling is reported to the operator dashboard within 500 milliseconds of the event occurring

VI. CONCLUSION

The development of an IoT-based Unmanned Ground Vehicle provides a scalable solution for army surveillance and border reconnaissance. The architecture addresses power consumption, communication stability, and physical security. Integrated sensors enable effective operation in hazardous environments. Thermal detection using the MLX90640 array and autonomous navigation via HC-SR04 ultrasonic sensors ensure consistent performance. The system successfully replaces traditional scouting methods with an automated robotic platform.

LoRa technology maintains a low-power telemetry link regardless of infrastructure availability. The MPU6050-based anti-tamper protocols provide a necessary layer of hardware security. This platform reduces human risk in conflict zones. Future research could investigate localized solar charging for extended missions. Swarm intelligence using LoRa mesh networking is another potential area for development. Collaborative autonomous units would allow for the monitoring of larger border perimeters with minimal human intervention.\

VII. ACKNOWLEDGMENT

The authors extend their sincere gratitude to the Department of Computer Science and Engineering at SRM Valliammai Engineering College for providing the necessary laboratory facilities, technical guidance, and institutional support required to complete this mini-project

VII. REFERENCES

[1]. Mandalik S. B., Gagare P., Tathe S., and Bhagwat V. (2025). Unmanned ground vehicle (UGV) for surveillance & reconnaissance, International Journal of Engineering Applied Sciences and Technology, (pp. 105–111).

[2]. Patel S., and Chen M. (2024). Thermal human detection in UGVs for hostile environments using edge AI, Journal of Real-Time Image Processing, (pp. 301–315).
[3]. Rodriguez L., and Yamamoto K. (2023). Multi-modal sensor integration in army UGVs for ISR missions, International Journal of Advanced Robotic Systems, (pp. 45–58).
[4]. Novak E., and Desai A. (2024). Anti-capture mechanisms in IoT scout vehicles using motion anomaly detection, IEEE Internet of Things Journal, (pp. 589–602).
[5]. Lee J., and Gupta P. (2024). Secure LoRa communication for scout UGVs with accelerometer-based tamper detection, IEEE Sensors Journal, (pp. 1142–1155).
[6]. Wang H., and Oliveira T. (2025). GPS-denied navigation for thermal-equipped military UGVs, Robotics and Autonomous Systems, (pp. 104–118).
[7]. Sharma A., and Kumar R. (2022). Low-power IoT architectures for remote military surveillance, IEEE Internet of Things Magazine, (pp. 34–40).
[8]. Gomez C., and Paradells J. (2019). Urban and remote automation networks using LoRaWAN: Opportunities and challenges, IEEE Communications Magazine, (pp. 112–118).
[9]. Nguyen T., and Smith J. (2021). Autonomous navigation for unmanned ground vehicles in off-road environments, Journal of Field Robotics, (pp. 445–462).
[10]. Zhang Y., and Li X. (2023). Thermal image processing for human detection in low-visibility conditions, Infrared Physics & Technology, (pp. 104–115).
[11]. Fernandez M., and Garcia L. (2022). Performance evaluation of ESP32 microcontrollers in IoT sensor nodes, Sensors Journal, (pp. 2110–2125).
[12]. Ali S., and Hassan M. (2021). Obstacle avoidance algorithms for UGVs using ultrasonic sensor fusion, Robotics and Autonomous Systems, (pp. 88–102).
[13]. Patel K., and Shah N. (2020). Power optimization techniques in battery-operated IoT devices, IEEE Transactions on Green Communications and Networking, (pp. 510–522).
[14]. Williams D., and Brown T. (2023). Anti-tamper and physical security mechanisms for remote IoT endpoints, IEEE Internet of Things Journal, (pp. 1820–1835).
[15]. Gupta R., and Singh A. (2022). Evaluation of sub-GHz LoRa transmission in dense forested environments, IEEE Wireless Communications Letters, (pp. 950–954).

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143