IntelliGuard: IoT-Enabled Autonomous Spybot Intelligence for Real-Time Surveillance in Next-Generation Security Applications

Dhruv Dhayal[1], Pratham Aggarwal[2] and Manzoor Ansari[3]

[1,2,3]*Department of Computer Science and IT,*
Institute of Information Technology & Management (IITM), GGSIP, University New Delhi, India
[1]*dhayaldhruv271@gmail.com*, [2]*aggarwalpratham2602@gmail.com*
,[3]*manzoor.ansari@iitmipu.ac.in*

Abstract
The rapid advancements in ubiquitous computing have made surveillance robots vital in military and security systems. IoT and sensor miniaturization enable new autonomous monitoring capabilities where traditional fixed installations or human operators prove ineffective. IntelliGuard, an ESP-32-based IoT surveillance robot, integrates camera streaming, motor-driven navigation, and centralized processing for military applications. The system provides autonomous mobility, real-time surveillance, and secure data transmission while remaining cost-effective. Radar and ultrasonic sensors enable precise obstacle detection within three meters. Field testing revealed performance variations under different environmental conditions, with optimal functionality in low-interference settings. Response latency remains minimal while IoT connectivity enables remote operation. Performance directly correlates with sensor precision and connection quality. Future developments will focus on more accurate sensors, stronger communication protocols, improved navigation for irregular obstacles, and enhanced filtering algorithms to minimize interference effects. This study establishes a foundation for advanced IoT-connected robotic surveillance systems in military applications.

Keywords: IoT Surveillance, Autonomous Spybot, Real-time Monitoring, Secure IoT Communication, Sensor Fusion Technology, Military Surveillance.

1 Introduction

While modern-day IoT applications are revolutionizing security and surveillance functions, organizations still lack comprehensive situational awareness in complex operational environments. Traditional surveillance systems face inherent limitations affecting their performance in real-world scenarios [1-3]. Unsupervised areas present significant security vulnerabilities that demand innovative technological solutions. Foundational research by Al-Fuqaha et al. (2015) established that IoT frameworks play a crucial role in overcoming these barriers through distributed sensor networks and real-time analytical processing [4]. Today's increasingly complex security landscape requires surveillance systems that minimize human supervision while maximizing detection accuracy and operational reliability

[5-6]. This paper presents IntelliGuard Ver.2, an autonomous IoT surveillance system designed to address the limitations of existing solutions through multi-sensor integration, adaptive artificial intelligence, and computational processing. The system architecture combines optical sensors, radar detection, and ultrasonic technologies within a unified framework, representing a significant advancement in IoT surveillance. IntelliGuard Ver.2 enables comprehensive environmental monitoring while reducing false positives through advanced pattern recognition algorithms and contextual analysis methodologies. The following sections detail the system's framework, components, implementation, and performance results across various operational scenarios.

1.1 Problem Definition

Traditional surveillance systems face significant operational constraints in dynamic or hazardous military environments. Fixed installations lack mobility and adaptability, while conventional surveillance robots are limited by communication infrastructure, operational range, and sensor critical factors for timely tactical responses.

Let the operational efficiency of a surveillance system be defined as:

$$\eta\text{surv} = \text{f}(\text{M}, \text{A}, \text{R})$$

Where mobility $M = \sum(i = 1\ to\ n)\alpha_i * m_i$ with α_i representing terrain-specific coefficients.

The convergence of IoT, AI, microcontrollers, and miniaturized sensors offers an opportunity to transcend these limitations. For a distributed IoT sensing network, system reliability is modeled as:

$$R_{sys} = 1 - \prod(i = 1\ to\ k)(1 - R_i)$$

Decision latency can be optimized through:

$$L_d = \min\left(\sum(i = 1\ to\ m)\left(\frac{D_i}{P_i}\right) + \sum(j = 1\ to\ n)\left(\frac{C_j}{B_j}\right)\right)$$

Where D_i represents data processing requirements, P_i is processing capability, $CC_j$is communication load, and B_j denotes bandwidth capacity.

This technological paradigm integrates multiple sensing modalities within unified architectures, providing unprecedented situational awareness while reducing human exposure to danger.

2 System Architecture: IoT-Driven Multi-Layered Security Framework for Real-Time Threat Detection and Adaptive Response

IntelliGuard Ver.2: newest version of IoT-based advanced security. It is meant to provide real-time surveillance capabilities like never before and unprecedented detection and automated intervention capabilities against threats. This type of multi-layered IoT architecture mounts a complete and almost seamless mechanism, highly precise threat mitigation across multiple environments of security, and is easily scalable integrated. The system capitalizes an IoT-enabled architecture for real-time surveillance and anomaly detection, and automated alerts, and further situational awareness from edge computing [7] and cloud analytic services [8]. This hybrid solution connects the low latency data processing and

decision-making while ensuring smooth communication among security nodes that are interconnected. Some outstanding innovations in the area include efficient IoT-based sensor networks, secure encrypted data transmission, and public remote device synchronization, which prove strong operational security posture in enterprise critical infrastructures. End-to-engage connectivity in IoT will enable an organization to monitor its activities in real-time, develop mobile-based remote access, and realize predictive risk estimates, thus enabling proactive security measures to be taken by the organization against imminent threats. Besides, it modularizes all the above into an IoT architecture within which IntelliGuard Ver.2 even enhances advanced sensor fusion, adaptive power management, and secured communication protocols to guarantee scalability and interoperability with existing security infrastructures. Furthermore, this layered system architecture provides improved resource utilization as well as real-time processing along with specific device management. Therefore, this solution represents a promising IoT implementation for smart surveillance and critical security applications. Through IoT-driven automation and advanced connectivity, IntelliGuard Ver.2 sets a new standard for next-generation security solutions in intelligent monitoring, real-time situational awareness, and adaptive threat response to evolving security challenges. As shown in Fig. 1(A) and 1(B), the system architecture of IntelliGuard Ver.2 illustrates the comprehensive data flow between components across all operational phases.

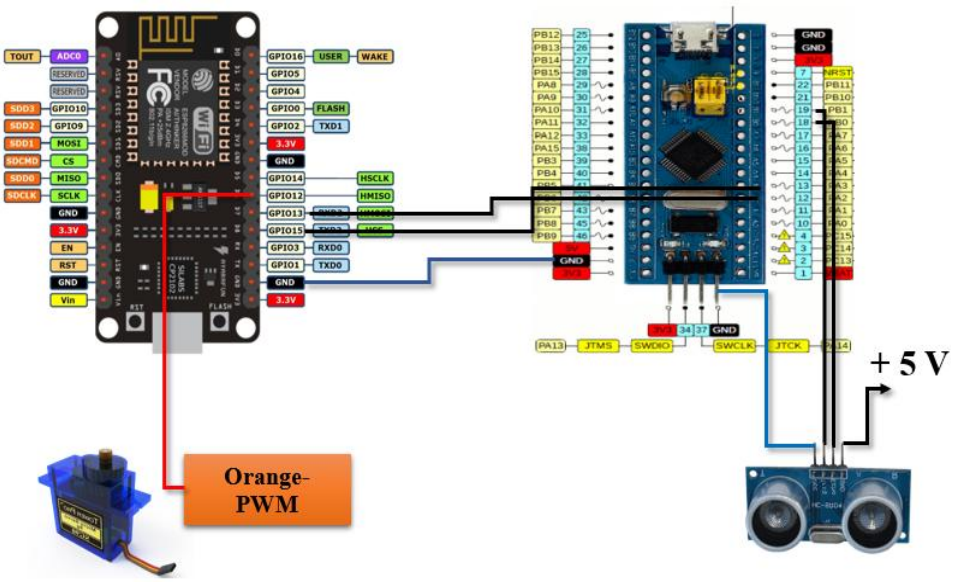

Figure (A)

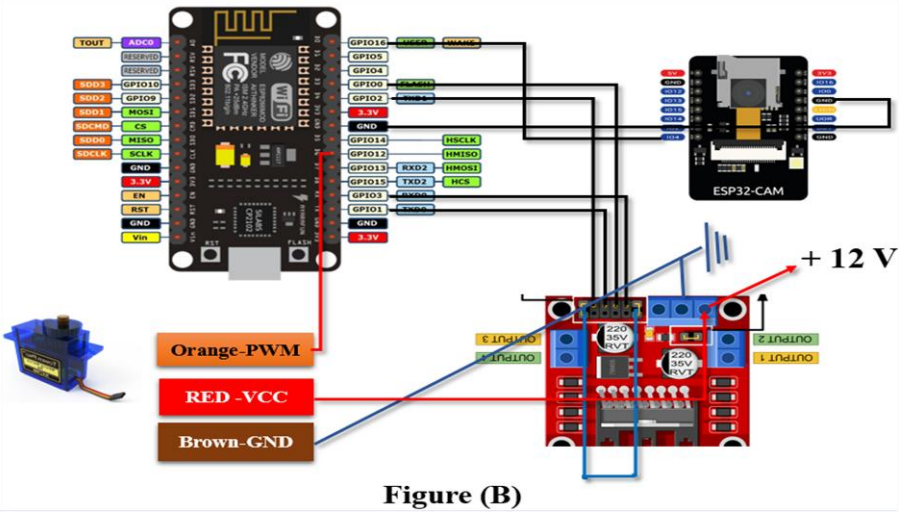

Fig 1 (A) (B): System Architecture of IntelliGuard Ver.2 Shows the proper working data flow between the components in every phase.

2.1 Components Used

The IntelliGuard surveillance system integrates advanced hardware to **gather environmental data, process real-time inputs, and enable secure communication** for autonomous operation. It utilizes a combination of **sensing, mobility, and communication technologies** to enhance situational awareness and adaptive response. The system's capabilities, including data acquisition, processing efficiency, and connectivity, are discussed in detail below, with hardware specifications outlined in Table 2: Hardware Components of the IntelliGuard Surveillance Robot**.**

Table 2: Components of the IntelliGuard Surveillance Robot

Components	Description
L298N Microcontroller	*Core controller managing data processing, sensor communication, and device operation.*
Wi-Fi module (ESP32 Cam)	*Captures and transmits real-time video for remote surveillance via the internet.*
Radar System	*Detects obstacles and moving objects, enhancing navigation and security.*
Ultrasonic Sensor	*Assists in obstacle detection and autonomous path planning.*
Servo Motor	*Controls the automated storage compartment for object handling.*
DC Motors (100 RPM)	*Enables multi-directional movement with speed control.*
Rechargeable Battery	*Ensures continuous power supply to all components. ~2000Mah*
Power Management Circuit	*Efficiently distributes power across all modules.*
NodeMCU (ESP8266)	*Acts as a backup controller for wireless communication and IoT integration.*

EMF Communication Module	*Allows short-range control (<4m) without internet or Wi-Fi.*
Private IP Integration	*Ensures secure, app-independent communication for controlling the robot.*
Wi-Fi Module (ESP-32 Built-in)	*Enables long-range remote control and live streaming.*

3 IoT-Enabled Surveillance System Implementation and Workflow

IntelliGuard is designed as a versatile spy bot for real-time monitoring and data acquisition in extreme environments including military operations, space exploration, borewells, mines, rescue operations, and firefighting scenarios. The system enables autonomous surveillance and threat detection in locations inaccessible or hazardous to humans. Advanced sensors and communication technologies allow seamless operation in extreme environments, as illustrated in Fig. 2.

Fig 2: Autonomous Spy Bot Prototype for Surveillance and Rescue Operations

The operational framework shown in Fig. 3 illustrates the interconnections between key subsystems of the motion-controlled rover: Power System, ESP-32 Control System, Motor & Movement System, Radar System, Headlight System, and Remote-Control Interface. The Power System forms the foundation of operations, comprising lithium-ion batteries, battery chassis, charger, and a power distribution board that stabilizes voltage for consistent delivery. At the core, the ESP-32 Control System functions as the central controller, processing inputs through its integrated camera, DPST switch, PL2303 TTL module, and WiFi capabilities. This controller interfaces with the Motor & Movement System, which enables mobility via DC motors on specialized terrain-handling wheels controlled by an L298D Motor Driver. Environmental awareness is enhanced by the Radar System, utilizing an HC-SR04 Ultrasonic Sensor mounted on an SG90 Servo Motor for rotational scanning. Sensor data is processed by an Arduino Nano and transmitted to a GUI for radar feedback. The Headlight System improves visibility in low-light conditions, controlled directly through the ESP-32 module. The Remote-Control Interface integrates all subsystems, allowing operators to regulate movement, speed, lighting, and monitor live camera streaming through a User Control & Web Interface using Static Private IP Protocol for secure communication with user

devices. This architecture demonstrates efficient power management and data exchange among components, creating a robust platform for autonomous surveillance in challenging environments.

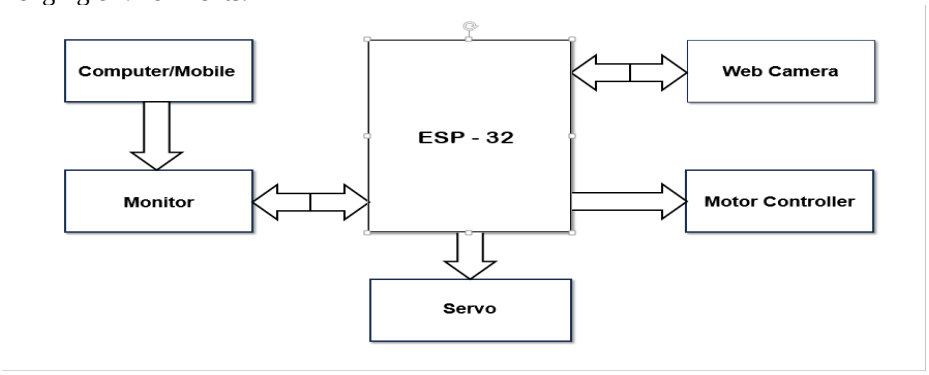

Fig 3: Manual Operational Design (Systematic)

4. Results and Discussion

The rapid development of robotics, automation, and IoT has imposed some impact on nearly all sectors from security, military, and industrial applications. The blending of autonomous surveillance technology has brought great changes to vital operations in terms of improving efficiency, safety, and accuracy. The study deals mainly with the successful building of the ESP-32-based surveillance robot for real-time monitoring and reconnaissance, proving applicable in many domains. The working model with on real-time monitoring system gives feedback to the mentioned used in **Fig.4** given below are:

Fig 4: System Workflow for Autonomous Surveillance and Rescue Operations

The robot uses a radar-based detection system to estimate the distance and angle of the object while simultaneously feeding the information in real-time to the GUI interface. This helps to detect obstacles based on gathered data object angle and distance.
Additionally, secure monitoring within the 4m range free from Wi-Fi/EMF using private IP, while long-range monitoring (1km) would need a network-enabled Wi-Fi network. Due to the design of the system for high-risk areas, it deals with problems of borewell rescues, coal mine monitoring, and pipeline inspections thereby protecting

human life during such hazardous conditions. Its mobility, powered by DC motors, allows it to go over various terrains in industry, military, and emergency applications [9, 10]. The implementation thus highlighted the possibility of low-cost applications run by AI where real-time data acquisition and remote access are of utmost importance. Future improvements will focus on the integration of high-precision sensors to further promote accuracy and adaptability. Additionally, these systems will be enhanced through the introduction of machine-learning-based sensor fusion, LiDAR, and SLAM (Simultaneous Localization and Mapping) furthering robot autonomy capabilities in dynamic and unpredictable environments [11]. This research offers a base for AI-driven surveillance robots that support their vital role in security, defense, and industrial automation as well as minimizing human intervention in life-threatening situations.

The operational workflow illustrated in Fig. 4 demonstrates the system's autonomous surveillance and rescue capabilities through integrated subsystem communication. As shown in Fig. 5 and Fig 6, a customized GUI interface was developed for tablet-based remote control of the system, properly integrated with a private IP connection (192.168.4.1) to ensure secure and responsive operation.

Fig 5: System Workflow for Autonomous Surveillance and Rescue Operations

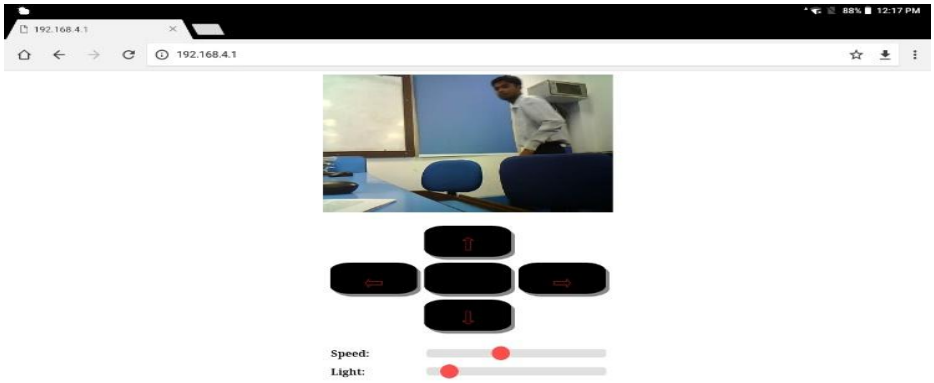

Fig 6: Designing GUI Interface on Tablet to remotely control the systematic model by proper Integration with Private IP connected 192.168.4.1

References

[1] E. Tikk-Ringas, Evolution of the Cyber Domain: The Implications for National and Global Security. Routledge, 2023.

[2] R. Zahira, P. Sivaraman, C. Sharmeela, and S. Padmanaban, Eds., IoT for Smart Grid: Revolutionizing Electrical Engineering. John Wiley & Sons, 2025.

[3] M. S. Islam, P. A. Ambresh, A. Birwal, M. S. R. Murty, S. Vyas, and V. Malhotra, "AI and IoT in Automation and Security: A Vision for Next Generation Applications," IUP J. Electr. Electron. Eng., vol. 17, no. 4, pp. 7–32, 2024.

[4] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[5] D. Chen and H. Liu (2023). Real-Time Data Processing Algorithms for IoT-Enabled Surveillance Applications. ACM Transactions on Sensor Networks, vol. 19, no. 2, pp. 15:1-15:28.

[6] T. Ribeiro, P. Oliveira, and M. Rodrigues, "Next-Generation Surveillance: Exploring the Intersection of Artificial Intelligence and Security," in Intelligent Systems Conference, Cham, Switzerland, July 2024, pp. 522–535.

[7] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," IEEE Access, vol. 8, pp. 85714–85728, 2020.

[8] S. Pashikanti, "Real-Time Data Streaming and Analytics: Architecting Solutions on Cloud Platforms," J. Artif. Intell. Mach. Learn. Data Sci., vol. 1, no. 1, pp. 2038–2040, 2023.

[9] D. Chen and H. Liu (2023). Real-Time Data Processing Algorithms for IoT-Enabled Surveillance Applications. ACM Transactions on Sensor Networks, vol. 19, no. 2, pp. 15:1-15:28.

[10] L. Zhang and F. Wang (2023). IoT-Based Surveillance Systems: Architecture, Challenges, and Future Directions. IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2154-2169.

[11] V. Garcia and N. Martinez (2023). Edge Computing Frameworks for Real-Time Video Analytics in Surveillance. Elsevier Future Generation Computer Systems, vol. 142, pp. 210-225.