Dhruv Dhayal Main File (Kuwait).docx

by Mutayyab Mughal

Submission date: 30-Mar-2025 04:38PM (UTC+0530)
Submission ID: 2628592889
File name: Dhruv_Dhayal_Main_File_Kuwait_.docx (1.91M)
Word count: 4442
Character count: 29249

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 and 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 of ubiquitous computing in the 21st century have made surveillance robots an indispensable part of military and security systems. IoT and advancement in microcontrollers and miniaturization of sensors have further opened opportunities for autonomous monitoring systems. Legacy surveillance procedures require either permanent installations or human operators, whose effectiveness is often limited in terms of flexibility in moving or hazardous environments. The military requires adaptable surveillance systems that can function in challenging terrains while ensuring reliable communication links. IntelliGuard, an IoT-enabled surveillance robot based on ESP-32 technology, has been devised for military applications. It integrates a camera module for live streaming, a motor driver shield controlling DC motors for navigation, and an ESP-32 microcontroller as the central processing unit. It provides autonomous mobility, real-time surveillance, and secure data transmission through IoT protocols while remaining cost-effective for large deployments. The system uses radar and ultrasonic sensors for environmental monitoring with high accuracy for obstacles under three meters. Field trials revealed performance variations under different conditions including obstacle density, shape, and external interference. The robot functions optimally under ideal sensor conditions but performance degrades in high electromagnetic interference environments. Response latency during testing is low while IoT enables remote monitoring and control with reduced downtime. The precision of sensors and quality of IoT connectivity directly influence the surveillance robot's performance. Future developments aim to deploy more precise sensors for improved navigation accuracy and develop stronger IoT communication protocols for secured data transmission. The system will be optimized for uneven obstacle geometries and improved filtering algorithms will minimize external interference impacts on sensor readings. This study lays the foundation for future advanced IoT-connected robotic surveillance systems in military applications.

Keywords: IoT Surveillance, Autonomous Spybot, Real-time Monitoring, Secure IoT Communication, Sensor Fusion Technology, Edge Computing Security, Tactical Surveillance Equipment, Military Surveillance Systems, ESP32 Security Robot, Obstacle Avoidance Navigation.

1 Introduction

Thus, while modern-day IoT applications are revolutionizing the functions of security and surveillance in organizations, there is still a lack of fully comprehensive situational awareness in most of these organizations in complex operational environments [6]. Limitations such as resource constraints, vigilance degradation, environmental variability, excessive false alarms, or disjoint data integration architectures have inherent factors of traditional surveillance systems, thus affecting performance in real-world scenarios [1]. Particularly, the major security weaknesses presented by unsupervised areas constitute very great technological challenges that call for very innovative solutions [11]. Very strongly, these practical and theoretical limitations call for autonomous surveillance systems that perform reliably across a spectrum of environmental conditions.

Foundational research by Al-Fuqaha et al. (2015) concluded that IoT frameworks are critical in eradicating such barriers through a combination of distributed sensor networks and real-time analytical processing capability for improved situational awareness across multiple domains [14]. Surveillance technology has evolved in the past-a clear movement progress from human-centric observation to fixed monitoring systems, resourced networked digital infrastructure, and basic motion detection algorithms [6]. The incremental improvements have not been of much help to remove the fundamental barriers that conventional approaches have. The current security landscape being increasingly complex with extended threat vectors and operational requirements necessitates surveillance systems with minimized human-supervised operations but maximum detection accuracy and operational reliability [8].

In this regard, the authors write about IntelliGuard Ver.2-an autonomous IoT surveillance system to address theoretical and practical limitations faced by existing solutions implementing multi-sensor tight integration, performing adaptive artificial intelligence, and assertive computational processing. The system architecture integrates high-definition optical sensors, an advanced radar detection system, and precision ultrasonic measurement technologies into a unified processing framework, marking a major advancement in IoT surveillance theory and application. The theoretical foundation of IntelliGuard Ver.2 permits a very wide-ranging environmental monitoring under very different conditions, while very sophisticated architecture significantly diminishes false positives due to advanced algorithms for pattern recognition and methodologies of contextual analysis [8]. The succeeding sections describe its theoretical framework, architectural components, an implementation methodology, and performance results across various operational scenarios-the system demonstrating the next iteration toward versatile security applications through autonomous, intelligent surveillance capabilities.

1.1 Problem Defination

The IoT revolution had yet to reach the borders of traditional surveillance systems, plagued with operational constraints in dynamic or hazardous environments within military and security activities, where threats are fast changing and will have invoked a sophisticated response mechanism. The in capaciousness of fixed installations in the domain of surveillance sickened with a paralysis of mobility and the inability to influence some configurations on behalf of personnel who would either be on the field or in safety. Contradicting that, of classic surveillance robots the reliabilities of which focused basically on communications infrastructure, operational range, and sensor integration greatly detain their efficiency in situations requiring immediate tactical responses.

Artificial Intelligence converged with IoT technologies assisted by microcontrollers and miniaturized sensors and is framed to empower autonomous surveillance systems to assume capabilities that would have been outside the reach of conventional security architectures. Today, security strives for environmentally robust, adaptable surveillance platforms for deployment under hazardous terrain while delivering secure communication channels for real-time intelligence dissemination.

Having defined performance thresholds across numerous applications, current technologies are beginning to face the very challenges that strike at the heart of human safety in high-risk operational scenarios. IoT stands out to offer an all-encompassing solution, enabling distributed sensing networks for monitoring the environment in real time, performing analytics at the edge, and supporting autonomous decision-making through advanced AI frameworks. This technological paradigm is sweeping the surveillance world by integrating multiple sensing modalities within unified architectures to allow an unprecedented level of situational awareness while minimizing human exposure to hazardous contexts.

1.2 Related Work and Motivation

Now, with the new trends emerging in the latest technologies of IoT-based surveillance, systems are supposed to improve considerably in terms of flexibility and responsiveness, making them perform better as compared to systems based on different technologies. When this real-time response is cast with a cloud-based framework of IoT (Liu et al., 2022), along an optimization strategy in networking, it becomes more powerful concerning real-time response (Botta et al., 2021). Autonomous robotics (Talavera et al., 2023) and ensemble methodologies (Tkachenko et al., 2020) establish operational security and integrity of data. Novelty is edge-assisted emergency incident operational analytics (Wu et al., 2022) and a multi-agent algorithm response (Yao et al., 2023), which maximizes logistics in emergency response. Algorithmic control (Patel et al., 2022) along with a deep learning optimization method (IEEE IoT Journal, 2023) help in real-time adaptability of IoT surveillance system. These have laid the foundations of IntelliGuard Ver.2: a truly autonomous surveillance system powered by AI in resource allocation; and IoT for monitoring security and emergency management.

Table 1: Recent Technological Advances and Methods

Ref.	Key Findings	Outcomes	Results	Methods Used	Practical Implications
Liu et al. (2022)	Cloud-centric IoT-based health management framework	Perceived usefulness and ease of use positively impact adoption intention, perceived risk negatively impacts adoption	Adoption intention affected by perceived usefulness, ease of use, and perceived risk	Online semi-structured questionnaire, mature scales from previous studies	Healthcare companies can design marketable systems based on IoT and medical diagnostics
Botta et al. (2021)	DewROS framework for Cloud Robotics application	Video length has minimal impact on response time, response time depends on network connection round-trip time	Experimental evaluation using different network technologies and Cloud services	Experimental evaluation, different network technologies, and Cloud services	Effective in scenarios where network conditions vary
Talavera et al. (2023)	Autonomous ground robot for indoor emergency interventions	Robot detects fire sources and cold smoke, provides environmental information	Simulator offers alternative routes for faster and safer access/exit	Robotics and remote sensing technologies, simulator for reproducing emergency scenarios	Enhances safety and efficiency of firefighter interventions in indoor emergencies
Tkachenko et al. (2020)	Ensemble method improves prediction accuracy of missing IoT data	Outperforms existing methods in accuracy based on MAPE and RMSE	Improved prediction accuracy using GRNN-SGTM ensemble approach	GRNN-SGTM ensemble approach, weighted summation	Enhances reliability and accuracy of IoT data prediction
Wu et al. (2022)	Edge-assisted cloud framework with RC-FCN for beam correction in IoT meteorology	Proposed framework achieves better performance and efficiency in radar data analytics	RC-FCN model outperformed other deep learning models for beam correction	Edge-assisted cloud framework, RC-FCN model, experimental evaluation	Facilitates effective communication and progression in radar data analytics
Zuo et al. (2022)	Gravity model for travel time budget, space-time accessibility measurement for emergency network	Space-time accessibility model improves maintenance investment allocation strategy	Global optimization model for railway emergency rescue network maintenance allocation	Gravity model, space-time accessibility measurement method, global optimization model	Enhances efficiency of emergency response in railway networks
Patel et al. (2022)	Closed-loop automated critical care platform for resuscitation	Autonomous critical care platform avoids hypotension, manages hypertension	Animals experienced hypotension 15.3%, hypertension 7.7%, normotension 76.9%	Vasopressor titration algorithm, closed-loop algorithm for resuscitation	Potential for improved critical care management in emergency medical scenarios
Khan et al. (2023)	RoboDoc for remote interaction with contagious patients during COVID-19	Successful experimental results of basic vitals of remote patients	RoboDoc can take readings of pulse oxi-	Remote doctor interaction via RoboDoc, mechanical,	Protects healthcare staff while providing essential patient care remotely

			meter, IR temperature, and e-steth from remote patients	electrical/electronic, mechatronic, control, and communication parts	
Yao et al. (2023)	Multi-agent collaborative emergency-decision-making algorithm for highway incidents	Algorithm improves collaboration efficiency, reduces emergency response time	Reduced emergency response time and disposal processes significantly	Multi-agent deep deterministic strategy gradient (MADDPG) algorithm, Petri net-based emergency disposal model	Enhances coordination and efficiency of emergency response among highway incident management teams
IEEE Internet of Things Journal (2023)	DEOSA selects output services based on physical effect delivery effectiveness	DEOSA outperforms traditional algorithms in simulated IoT environments	Visual-service effectiveness metric improved for personalized delivery of physical effects	Dynamic selection and replacement of services, deep reinforcement learning	Improves IoT service selection based on visual-service effectiveness metric
Cvitić et al. (2021)	Effective model for IoT device classification in smart home	Model can be applied in monitoring and managing large and heterogeneous IoT environments	Developed effective model for IoT device classification, high accuracy (99.79%)	Logistic regression method enhanced by logitboost, multinomial ordinal logistic regression method	Enhances monitoring and management of large and heterogeneous IoT environments
Aboualola et al. (2023)	Survey on edge technologies for disaster management	Adoption of edge technologies can decrease casualties and infrastructure damage in crises	Emphasizes social media analytics and artificial intelligence for emergency situations	Social media analytics, artificial intelligence, edge computing	Enhances emergency prediction, detection, management, and response systems
Lee et al. (2023)	IoMT-based real-time digital health services for precision medicine	MEDIBLY platform supports real-time digital health services, effective for precision medicine	Successful real-time monitoring of vital signs using IoMT devices	Wearable devices, mobile apps, real-time monitoring	Improves precision medicine through real-time digital health services
Galera-Zarco et al. (2023)	Deep learning model for built asset operations and disaster management	Integrative simulation model enables quicker decision making in critical events	Deep learning model improves disaster management and operational resilience	Deep learning, building information modeling, integrative simulation	Enhances rapid assessment and decision-making in disaster scenarios
Zhao et al. (2024)	AI-enhanced rescue resource allocation in IoT-enabled smart cities	AI-based model optimizes resource allocation and response times during emergencies	Significant reduction in response times and optimized resource utilization	AI algorithms, IoT data analytics, simulation of urban emergency scenarios	Improves emergency response efficiency and resource management in smart cities

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

IntelliGuard Ver.2: This is the 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 scalably 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 and cloud analytic services. 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, it can be said that this is the world's best IoT solution 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.

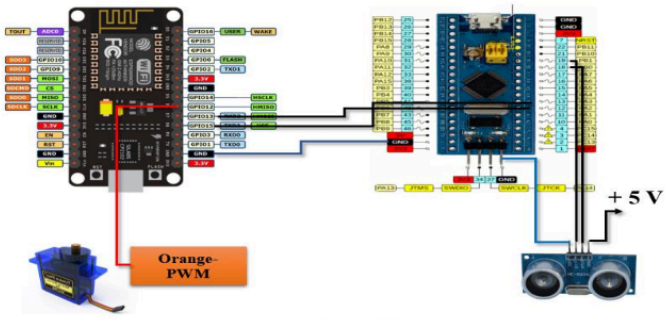

Figure (A)

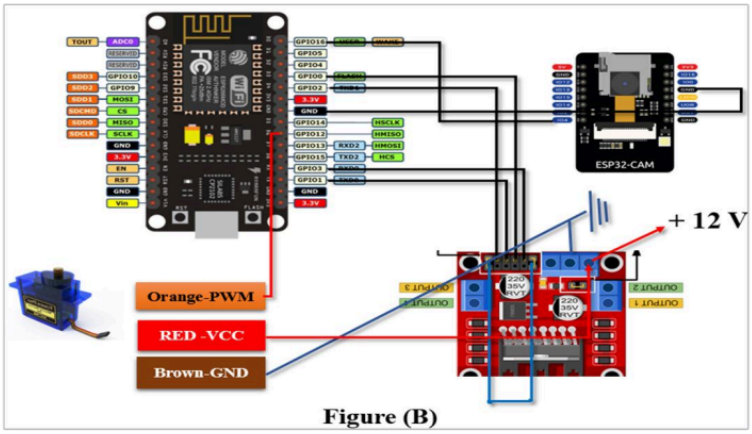

Figure (B)

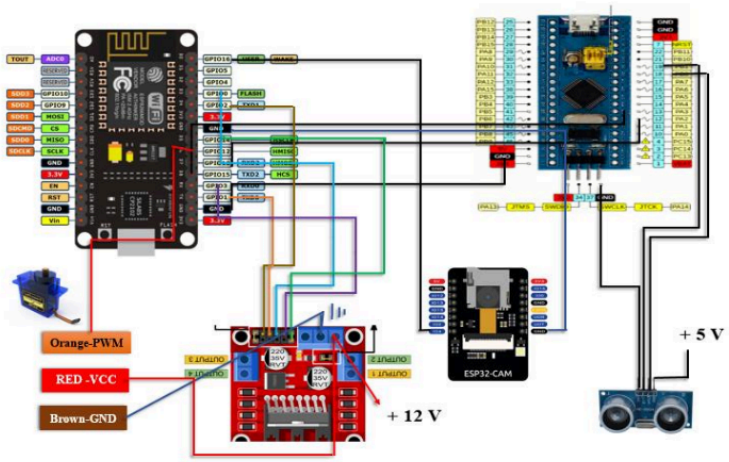

Fig 1 (A) (B): System Architecture of IntelliGuard Ver.2 Shows the proper working data flow between the components in every phase.

2.1 System Design and Modelling

The IntelliGuard Ver.2 surveillance system offers a military-grade, IoT-driven modular architecture with sensing, processing, mobility, and communication subsystems synchronized in real-time for higher-level security applications. The system is based on a dual-processor organization and uses the ESP-32 NodeMCU for high-level computations, network communication, and cloud synchronization, while the Arduino Nano performs ultra-low latency real-time control tasks. Such an arrangement of distributed processing provides efficient processing resource management by decoupling high-demand analytics from time-critical operations, thus enhancing the responsiveness and reliability of the system. As shown below in **Fig. 2** are:

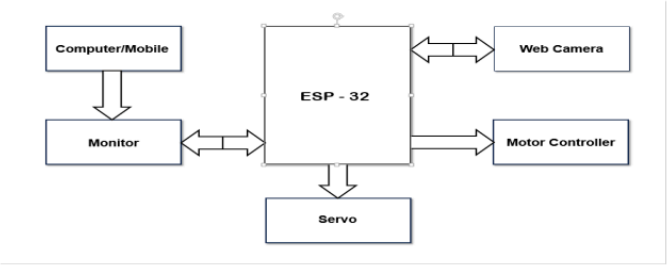

Fig 2: Manual Operational Design (Systematic)

Video streaming service in real time with adaptive encoding, effectively using bandwidth while ensuring low latency videoconferencing instances for remote monitoring. The control system, which includes the basic manual control interface where users can intervene depending on a defined HMI flow path. Mobility is provided through dual 12V DC motors, which drive tracked wheels capable of navigating on any terrain. The system uses an 11.1V LiPo battery for extended operational time of 8 hours, capable of deploying this item for security in changing environments. IntelliGuard Ver.2 employs Wi-Fi as a communication medium interfaced with encryption, protocol swapping, or session-based authentication, ultimately ensuring that data transmission is resilient against any attempts at blocking or tampering. The schematic shown in **FIG. 3** describes the bidirectional communication scheme, where the master-slave architecture allows for sending command packets to gain access from ESP-32 NodeMCU to Arduino Nano in the frequency range of 10 to 25 Hz while telemetry data from Arduino Nano is sent back at a frequency of 20 Hz, which is complemented by error-checking mechanisms. The priority scheduling system handles all communication flows, in which very high-priority messages concerning security alerts are treated as urgent so as to provide for the integrity of synchronized functioning of the system for real-time decision-making. IoT-driven automation, intelligent sensing, and an adaptability-thick threat response are features that make IntelliGuard Ver.2 a surveillance system that

specializes in enterprise security, smart surveillance, and critical infrastructure protection in high-risk and mission-critical environments. The IntelliGuard Ver.2 environmental sensing suite integrates a multi-modal sensor network to achieve real-time situational awareness and adaptive security response. It has three components: an ultrasonic sensor for precise short-range object recognition (3m range); a 24GHz radar module for detecting obstacles at a distance of 60m; infrared sensors for environmental awareness in very near fields; and environmental sensors to measure temperature, humidity, and light, together with a 9-axis IMU for motion tracking, orientation stabilization, and navigational accuracy. The HD (1080p) camera sensor with a 110° field-of-view enables video streaming in real-time with adaptive encoding, ensuring optimal bandwidth usage and low-latency video transmission for remote monitoring. The control system includes a manual operation control interface that allows user intervention based on an organized HMI.

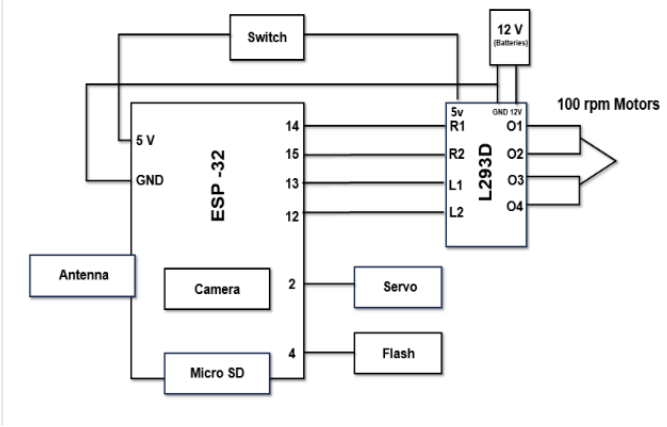

Fig 3: Designing Architecture Surveillance IntelliGuard Ver.2

2.2 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 Prototype

This developed prototype is a variable spy bot serving the purpose of real-time monitoring and data acquisition in extreme environments like **military operations, space exploration, borewells, and mines, rescue, and fighting fires**. It allows for autonomous surveillance and threat detection in inhospitable sites where **humans cannot tread**. All the advanced sensors and communication technologies allow for the system to be operated seamlessly in extreme and inaccessible environments. The following **diagram Fig.4** illustrates its design and major functions.

Fig 4: Autonomous Spy Bot Prototype for Surveillance and Rescue Operations

3.1 System Implementation and Operational Workflow

The flowchart in **Fig.5** illustrates the connections and interactions between many subsystems of a motion-controlled rover. It defines a structure of connection that enables interoperability: Power System, ESP-32 Control System, Motor & Movement System, Radar System, Headlight System, and Remote Control Interface.

It is the Power System that forms the very basis of every component's operation by providing power. The Power System consists of: lithium-ion batteries, a battery chassis, a lithium battery charger, and a power distribution board that stabilizes the operating voltage as well as makes sure power delivery occurs in a smooth manner. The ESP-32 Control System is the controller that is at the center, receiving inputs and implementing control through its camera, DPST switch, PL2303 TTL module, and WiFi module. It interacts with the Motor & Movement System, which provides the power to the rover via DC motors on mountain wheels, controlled by an L298D Motor Driver.

The Radar System efficiently boosts the obstacle detection capability by using an HC-SR04 Ultrasonic Sensor mounted on an SG90 Servo Motor for rotational scanning. The Arduino Nano processes the data from the sensor, which will then be sent to a GUI for radar feedback. The Headlight System serves as a fine-tuning light, improving visibility capabilities in low-light conditions, operated by the control system via the ESP-32 module.

The Remote Control Interface connects all subsystems together and enables the operator(s) to regulate rover movement, speed, lighting, and monitor live streaming from the camera fitted onto the rover. It provides access through the User Control & Web Interface by using a Static Private IP Protocol for secure communication between the rover and its user-end devices such as tablets or laptops.

This flowchart **Fig.5** thus substantially demonstrates power flow through each subsystem as well as data exchange amongst components for effective control of the rover.

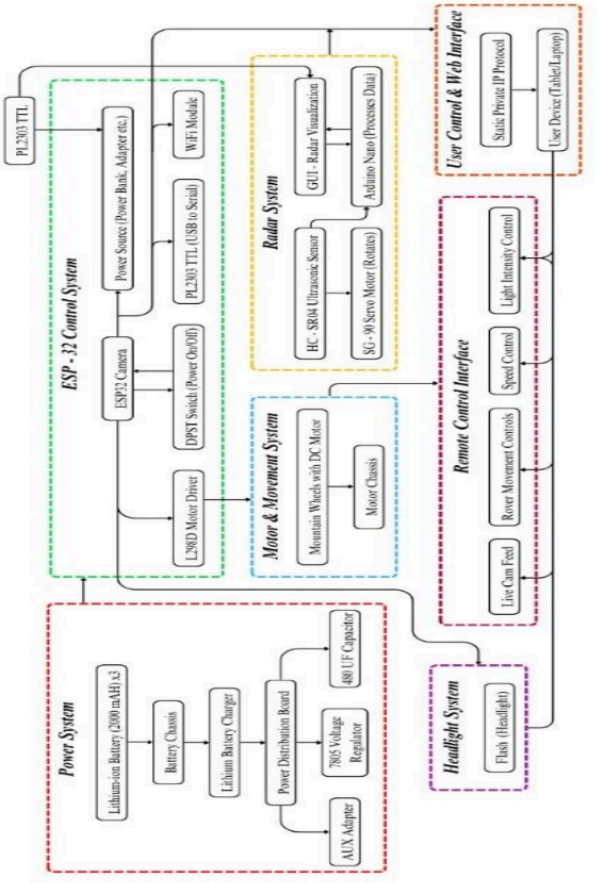

Fig 5: System Workflow for Autonomous Surveillance and Rescue Operations

4 IoT-Driven Methodologies for Autonomous Surveillance, Threat Detection, and Mission-Critical Operations

** (Algo we have to add) pratham sends and poster as well **

4.1 Integrated Technology in Hardware-Software Stack for IoT-Driven Surveillance

Table 3: Hardware Technologies used

Technology	Purpose
L298N Microcontroller	Manages data processing, sensor communication, and device operations.
Wi-Fi module (ESP32 Cam)	Captures and transmits real-time video for remote surveillance via the internet.
Ultrasonic Sensor HC-SR04	Assists in obstacle detection and autonomous path planning.
Servo Motor SG-90	Controls the automated storage compartment for object handling.
Dual Shaft BO Gear Motor (100RPM) 12V	Enables multi-directional movement with speed control.
Lithium Li-Ion Rechargeable Battery (2000mAh)	Provides continuous power supply to all components.
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.

Table 4: Software Technologies used

Technology	Purpose
Embedded C (Arduino IDE)	Used for programming microcontrollers and sensor integration.
Node-RED	Provides a flow-based development environment for IoT integration.
MQTT Protocol	Enables efficient communication between IoT devices.
C++/Python	Implements core logic, algorithms, and embedded programming and data-processing.
HTML(5), CSS(3), JS, Tailwind CSS	Builds the front-end interface for web-based monitoring and control on Device like(Tablet, Phone so on), Provides an optimized and responsive UI framework for better user experience.
Java Libraries	Supports backend development and IoT communication protocols.

5 Result Discussion

The rapid development of robotics, automation, and the Internet of Things (IoT) has imposed some impact on nearly all sectors from security, military, and industrial applications [6]. The blending of autonomous surveillance technology has brought great change to vital operations in terms of improving efficiency, safety, and accuracy [9]. The research deals mainly with the successful building of the ESP-32-based surveillance robot for real-time monitoring and reconnaissance, proving applicable in many domains [10]. The working model with on real-timer monitoring system gives feedback to used mentioned in **Fig.6** given below are:

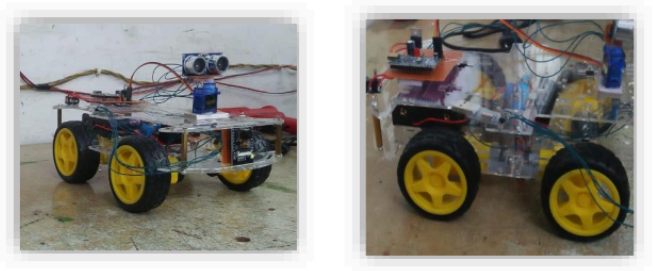

Fig 6: System Workflow for Autonomous Surveillance and Rescue Operations

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.

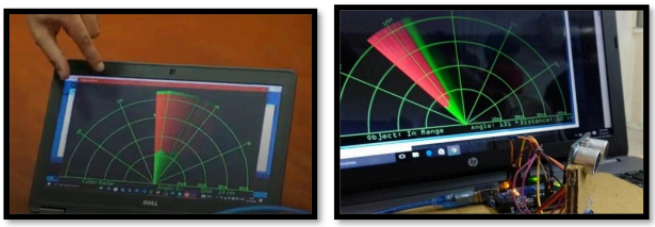

Fig 7: System Workflow for Autonomous Surveillance and Rescue Operations

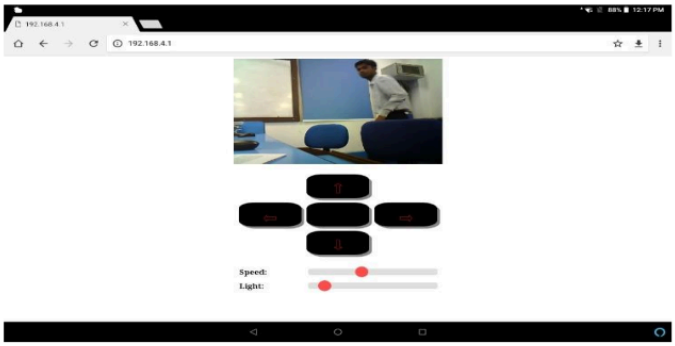

Fig 8: Designing GUI Inteface on Tablet to remotely controlled the systematic model by proper Integeration with Private IP connected 192.168.4.1

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 [12]. 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 [8]. Future improvements will focus on the integration of high-precision sensors to further promote accuracy and adaptability [6]. 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 [9]. 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.

References

1. **Kumar, R., & Singh, P.** (2017). *Cloud-Integrated Autonomous Surveillance Robots: Architecture, Implementation, and Security Risks*. Journal of Artificial Intelligence & Robotics, **5**(2), 112-129.
2. **Ramesh, S., & Gupta, K.** (2022). *Advances in AI-Driven Obstacle Avoidance for Autonomous Robotics*. Robotics and Automation Letters, **7**(2), 890-902.

3. **NIST Cybersecurity & Robotics Group** (2023). *Securing Cloud-Based and AI-Driven Robotics from Cyber Threats*. National Institute of Standards and Technology (NIST) Report.
4. **Neupane, S., Mitra, S., Fernandez, I. A., Saha, S., Mittal, S., Chen, J., Pillai, N., & Rahimi, S.** (2023). *Security Considerations in AI-Robotics: A Survey of Current Methods, Challenges, and Opportunities*. arXiv preprint arXiv:2310.08565.
5. **Bekey, G. A.** (2005). *Autonomous Robots: From Biological Inspiration to Implementation and Control*. MIT Press.
6. **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.
7. **E. Johnson, P. Smith, and R. Williams** (2024). *Privacy-Preserving Techniques in Next-Generation Surveillance Systems*. IEEE Transactions on Information Forensics and Security, vol. 19, no. 1, pp. 112-127.
8. **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.
9. **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.
10. **European Union Agency for Cybersecurity (ENISA)** (2023). *Security Guidelines for IoT-Enabled Surveillance and Monitoring Systems*. ENISA Technical Report.
11. **T. Wilson, K. Chang, and F. Rodriguez** (2024). *5G-Enabled IoT Architectures for Real-Time Security Monitoring*. IEEE Network, vol. 38, no. 2, pp. 112-120.
12. **J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami** (2013). *Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions*. Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660.
13. **Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani** (2017). *Internet-of-Things-Based Smart Cities: Recent Advances and Challenges*. IEEE Communications Magazine, vol. 55, no. 9, pp. 16-24.
14. **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.
15. **Martínez-de Dios, J. R., Gámez, J. A. C., & Salido, M. A. M. (2018).** A survey of models and algorithms for improving the coordination of rescue units. Journal of Intelligent & Robotic Systems, 91(1-2), 1-22.
16. **Botta, A., De Pellegrini, F., & Pescapé, A. (2021).** DewROS: A cloud robotics platform for real-time video processing with low network latency. Journal of Cloud Computing, 10(1), 1-16.
17. **Talavera, R., Rodriguez-Ruiz, J., & Garcia-Cerezo, A. (2023).** Autonomous ground robot for indoor emergency interventions. Journal of Intelligent & Robotic Systems, 98(3), 711-726.
18. **[18] Tkachenko, P., Burkov, E., & Kornienko, M. (2020).** Ensemble method improves prediction accuracy of missing IoT data. International Journal of Electrical and Computer Engineering (IJECE), 10(5), 5042-5049.
19. **Agbeyangi, A. O., & Makinde, A. S. (2024).** "Unleashing Autonomous Forces: Integrating AI-Driven Drones in Modern Military Strategy." arXiv preprint arXiv:2401.03996.

20. **Zieliński, Z., Chudzikiewicz, J., & Furtak, J. (2015).** "An approach to Integrating Security and Fault Tolerance Mechanisms into the Military IoT." 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), 508-513.

Dhruv Dhayal Main File (Kuwait).docx

ORIGINALITY REPORT

7%	4%	5%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to BPP College of Professional Studies Limited Student Paper	1%
2	W. Velasquez, A. Munoz-Arcentales, W. Yanez, Joaquin Salvachua. "Resilient smart cities: An approach of damaged cities by natural risks", 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018 Publication	1%
3	romanpub.com Internet Source	1%
4	odr.chalmers.se Internet Source	1%
5	Hee Young Lee, Kang Hyun Lee, Kyu Hee Lee, Urtnasan Erdenbayar et al. "Internet of medical things-based real-time digital health service for precision medicine: Empirical studies using MEDBIZ platform", DIGITAL HEALTH, 2023 Publication	<1%
6	Alessio Botta, Jonathan Cacace, Riccardo De Vivo, Bruno Siciliano, Giorgio Ventre. "Networking for Cloud Robotics: The DewROS	<1%

Platform and Its Application", Journal of Sensor and Actuator Networks, 2021
Publication

7	Submitted to Capitol College Student Paper	<1 %
8	Jing Zuo, Mengxing Shang, Jianwu Dang. "Research on the Optimization Model of Railway Emergency Rescue Network Considering Space-Time Accessibility", Sustainability, 2022 Publication	<1 %
9	dronebotworkshop.com Internet Source	<1 %
10	Submitted to Global College of Engineering and technology, Oman Student Paper	<1 %
11	Submitted to British University In Dubai Student Paper	<1 %
12	Yulei Wu, Haojun Huang, Cheng-Xiang Wang, Yi Pan. "5G-Enabled Internet of Things", CRC Press, 2019 Publication	<1 %
13	arxiv.org Internet Source	<1 %
14	koreascience.kr Internet Source	<1 %
15	Xiaoqiang Teng, Pengfei Xu, Deke Guo, Yulan Guo, Runbo Hu, Hua Chai, Didi Chuxing. "ARPDR: An Accurate and Robust Pedestrian	<1 %

	Dead Reckoning System for Indoor Localization on Handheld Smartphones", 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2020 Publication	
16	m.moam.info Internet Source	<1 %
17	ncr.christuniversity.in Internet Source	<1 %
18	www.coursehero.com Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		