

Rocket Launch with Google Assistant and IOT

Manamohana M

*Dept. of Computer Science and Engineering
(IoT, Cyber Security including Blockchain Technology)
Maharaja Institute of Technology Mysore
Karnataka, India
manamohanam8277@gmail.com*

Keerthan gowda T R

*Dept. of Computer Science and Engineering
(IoT, Cyber Security including Blockchain Technology)
Maharaja Institute of Technology Mysore
Karnataka, India
keerthangowda989@gmail.com*

Priya M L

*Dept. of Computer Science and Engineering
(IoT, Cyber Security including Blockchain Technology)
Maharaja Institute of Technology Mysore
Karnataka, India
priyam020105@gmail.com*

Seema C K

*Assistant Professor
Dept. of Computer Science and Engineering
(IoT, Cyber Security including Blockchain Technology)
Maharaja Institute of Technology Mysore
Karnataka, India
seema_csic@mitmysore.in*

Abstract— Conventional rocket ignition systems require operators to remain in close physical proximity to the launcher, which increases the risk of burns, accidental ignition, and operational failure due to misfires. Recent advancements in Internet of Things (IoT), cloud computing, and voice-enabled automation provide new opportunities to improve safety and reliability in such safety-critical systems. This paper presents the design and implementation of a voice-controlled rocket launcher using Google Assistant, Sinric Pro cloud platform, and an ESP8266 microcontroller. User voice commands are processed through a cloud-based communication layer and transmitted securely to the embedded controller, which regulates launcher orientation and initiates ignition using a relay-controlled nichrome wire heating mechanism. Electrical isolation, time-restricted ignition, and remote operation are employed to ensure safe and reliable system behavior. Experimental evaluation demonstrates low command latency, accurate execution, and consistent ignition performance under controlled conditions. The proposed system illustrates the feasibility of integrating cloud-assisted voice control with embedded ignition mechanisms and serves as a practical framework for educational, experimental, and safety-oriented automation applications.

I. INTRODUCTION

Internet of Things (IoT) technology enables physical devices to connect to the internet, allowing real-time data exchange, remote control, and intelligent operation with minimal human intervention. When integrated with cloud computing, IoT systems achieve enhanced scalability, reliability, and centralized command execution, making them suitable for applications such as smart homes, healthcare, industrial automation, and safety-critical systems. Alongside IoT advancements, voice-enabled intelligent assistants such as Google Assistant, Amazon Alexa, and Siri have emerged as effective human-machine interaction platforms. By leveraging natural language processing and speech recognition, these systems enable hands-free control and improved accessibility. The integration of voice assistants with IoT platforms has resulted in intuitive automation systems that reduce operational complexity. Despite these advancements, many safety-critical

applications, including rocket ignition systems, continue to rely on conventional manual control mechanisms. Such systems often require operators to remain close to the launcher during ignition, increasing the risk of injury due to accidental ignition or system failure. Existing remote-control solutions offer limited improvement, as they still require manual interaction and often lack intelligent validation and multi-layered safety mechanisms. The integration of cloud-assisted voice control provides a promising solution by enabling secure, remote, and handsfree operation. Cloud platforms validate commands and ensure controlled execution, while embedded systems handle real-time actuation. In ignition applications, nichrome wire is commonly used due to its predictable heating behavior; however, safe operation requires electrical isolation between control logic and high-current circuits. This work presents a voice-controlled rocket launcher using Google Assistant, Sinric Pro, and an ESP8266 microcontroller. The system enables safe launcher orientation and ignition through relay-controlled nichrome wire heating, incorporating arm/disarm logic, time-restricted activation, and electrical isolation. The proposed architecture ensures safety, scalability, and modularity, making it suitable for educational and experimental safety-critical applications.

II. RELATED WORK

Research related to the proposed system spans multiple domains, including IoT-based automation, cloud-assisted control systems, voice-enabled human-machine interaction, and embedded ignition mechanisms. This section reviews relevant work in these areas and highlights the research gap addressed by this paper.

A. IoT-Based Automation Systems

IoT-based automation has been widely applied in smart homes, industrial control, healthcare monitoring, and defense-related applications. Numerous studies demonstrate that IoT enables real-time monitoring, remote control, and intelligent decision-making through the integration of embedded devices and cloud

platforms. Cloud connectivity enhances system scalability, flexibility, and secure data exchange. Cloud-assisted IoT systems have been shown to reduce human intervention in hazardous environments. In industrial automation, remote operation of machinery improves worker safety and operational efficiency. Similar techniques are used for monitoring critical infrastructure where physical access is unsafe. However, many existing systems rely on mobile or web interfaces, which still require physical user interaction and may not be suitable for high-risk scenarios.

B. Voice-Controlled Systems and Virtual Assistants

Voice-controlled systems have gained attention due to advancements in natural language processing and artificial intelligence. Virtual assistants such as Google Assistant and Amazon Alexa are commonly used in smart home applications to control lighting, appliances, and security systems. Studies report improved usability and accessibility through hands-free interaction. Voice-enabled automation reduces cognitive load and is useful in environments where manual interaction is unsafe or inconvenient. However, most voice-controlled systems are designed for low-risk applications. Limited research explores voice control in safety-critical systems such as ignition mechanisms, where challenges include accidental activation, latency, authentication, and reliability.

C. Cloud-Based Control Platforms

Cloud platforms provide centralized processing, authentication, and device management in IoT systems. Research shows that cloud-based architectures can validate commands, manage device states, and enable reliable communication using protocols such as MQTT and WebSockets. By separating user interfaces from hardware components, cloud intermediaries improve system reliability and allow additional safety checks before actuation. However, cloud dependency introduces challenges such as network latency and availability, requiring fault-tolerant and fail-safe system design.

D. Embedded Ignition and Heating Mechanisms

Embedded ignition systems are commonly used in aerospace and experimental rocketry. Nichrome wire is widely employed as an ignition element due to its high electrical resistance and predictable heating behavior. Studies emphasize the importance of electrical isolation between microcontrollers and high-current ignition circuits, with relay-based isolation being a common solution. Most existing ignition systems are manually triggered or use simple remote switches. These systems lack intelligent validation, cloud connectivity, and voice-based interaction, limiting their safety and automation capabilities.

E. Identified Research Gap

Although significant research exists in IoT automation, voice-controlled systems, cloud platforms, and embedded ignition mechanisms individually, limited work has focused on integrating these technologies into a unified, safety-oriented architecture. Most voice-controlled systems are restricted to low-risk applications, while ignition systems lack intelligent automation and remote accessibility. The proposed work

addresses this gap by presenting a **cloud-assisted, voice-controlled rocket launcher** that integrates Google Assistant, Sinric Pro, and ESP8266 with a relay-based nichrome wire ignition system. This approach demonstrates the safe application of voice automation in a safety-critical embedded system.

III. PROBLEM STATEMENT

Rocket ignition systems are safety-critical due to high temperatures and combustible materials involved during launch. Conventional ignition methods require operators to remain close to the launcher, increasing the risk of burns, accidental ignition, and human error. Although remote control methods exist, many lack intelligent automation, secure command validation, and reliable safety mechanisms. Voice-controlled automation can reduce human involvement in hazardous environments; however, most existing voice-based systems are designed for low-risk applications and do not adequately address safety-critical requirements such as command authentication, latency, and electrical isolation. Additionally, traditional ignition mechanisms often lack proper isolation between control and high-current circuits, increasing the risk of unsafe operation. Hence, there is a need for a **safe, reliable, and voice-controlled rocket ignition system** that enables remote operation, minimizes human exposure, and ensures controlled ignition through secure cloud communication and embedded safety mechanisms.

IV. SYSTEM ARCHITECTURE

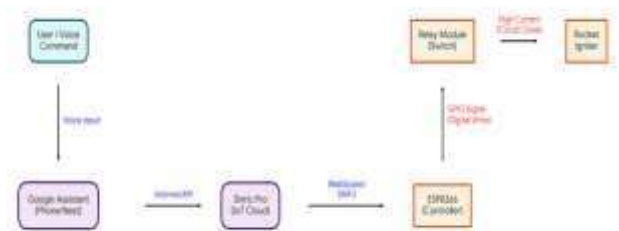


Fig. System architecture showing voice command flow from Google Assistant to ESP8266-controlled relay ignition.

The proposed system architecture is designed to provide safe, reliable, and remote control of a rocket launcher using cloud-based IoT and embedded technologies. The architecture follows a modular and layered approach, ensuring scalability, fault isolation, and ease of implementation. It integrates voice control, cloud communication, embedded processing, and actuation mechanisms into a unified framework. The system is composed of four main layers: the **Voice Interface Layer**, **Cloud Communication Layer**, **Control Layer**, and **Actuation Layer**. Each layer performs a specific function and interacts with adjacent layers through well-defined interfaces.

A. Voice Interface Layer

The Voice Interface Layer provides user interaction with the system. Google Assistant is used to capture voice commands issued by the user. These commands are predefined to avoid ambiguity and accidental activation. The voice interface

converts spoken commands into structured digital requests that are forwarded to the cloud platform for further processing.

B. Cloud Communication Layer

The Cloud Communication Layer is implemented using the Sinric Pro cloud platform. It acts as an intermediary between the voice interface and the embedded controller. This layer authenticates user commands, manages device states, and securely transmits validated commands to the ESP8266 microcontroller over the internet. The use of cloud-based communication enables remote access, command validation, and system scalability.

C. Control Layer

The Control Layer consists of the ESP8266 NodeMCU microcontroller, which serves as the central processing unit of the system. It receives commands from the cloud platform via Wi-Fi and executes control logic based on the system state. The controller performs safety checks such as arm/disarm verification before allowing any ignition-related operation. It also generates control signals for peripheral devices such as the servo motor and relay module.

D. Actuation Layer

The Actuation Layer includes the physical components responsible for mechanical movement and ignition. A servo motor is used to adjust the launcher angle, allowing controlled orientation before ignition. The ignition mechanism employs a relay-controlled nichrome wire heating system. The relay provides electrical isolation between the low-power control circuitry and the high-current ignition circuit, ensuring safe operation. An external power supply is used to energize the nichrome wire for controlled heating and ignition.

V. IMPLEMENTATION DETAILS

This section describes the practical implementation of the proposed voice-controlled rocket launcher, including hardware integration, software development, cloud configuration, and safety mechanisms. The implementation emphasizes reliability, electrical isolation, and secure command execution.

A. Hardware Implementation

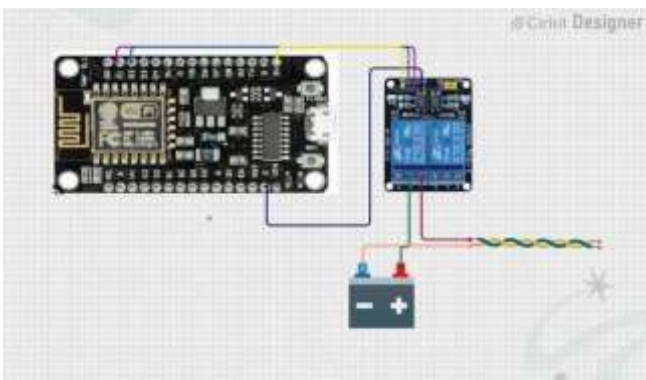


Fig. Hardware circuit diagram of the ESP8266-based relay-controlled nichrome wire ignition system.

The core hardware component of the system is the **ESP8266 NodeMCU** microcontroller, selected for its built-in Wi-Fi capability, low power consumption, and compatibility with IoT platforms. The microcontroller interfaces with a **servo motor** to control the launcher's orientation using pulsewidth modulation (PWM) signals. The ignition subsystem employs a **nichrome wire heating element**, which is energized through a **relay module**. The relay provides galvanic isolation between the low-power control circuitry and the high-current ignition circuit, protecting the microcontroller from electrical stress. An **external power supply** is used to drive the nichrome wire, ensuring sufficient current for ignition without affecting controller stability. All hardware connections are designed to minimize signal interference and ensure safe operation. Proper grounding and insulation are maintained to prevent short circuits and unintended activation.

B. Software Implementation

The firmware for the ESP8266 is developed using the **Arduino IDE**. The program initializes Wi-Fi connectivity, establishes communication with the **Sinric Pro cloud platform**, and continuously listens for incoming control commands. Event-driven programming is employed to ensure responsive command handling. The control logic includes state-based execution, where ignition commands are processed only when the system is in an armed state. Timers are implemented to limit the duration of relay activation, preventing overheating of the nichrome wire. Error handling routines manage network disconnections and ensure the system returns to a safe idle state when faults are detected.

C. Cloud and Voice Integration

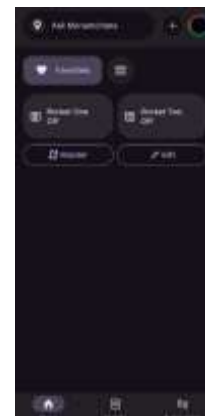


Fig. Google Assistant application interface showing cloud-based control of rocket ignition devices.

The **Sinric Pro cloud platform** is configured to integrate with **Google Assistant**, enabling voice-based command input. Predefined voice commands are mapped to specific device actions, reducing ambiguity and preventing accidental triggers. The cloud layer authenticates commands and forwards them securely to the ESP8266 using WebSocket communication.

D. Safety and Reliability Measures

Multiple safety mechanisms are incorporated into the implementation. These include arm/disarm logic, electrical isolation through relay switching, time-restricted ignition control, and automatic shutdown after execution. Together, these measures ensure reliable operation and minimize risks associated with ignition-based systems.

VI. SECURITY ANALYSIS

Security is a critical consideration in cloud-assisted, voicecontrolled embedded systems, particularly when applied to safety-critical operations such as rocket ignition. The proposed system incorporates multiple layers of security to prevent unauthorized access, accidental activation, and malicious interference. At the user interaction level, access to the system is restricted through the authentication mechanisms provided by the voice assistant platform. Voice commands are processed only from authorized user accounts linked to the cloud service, reducing the risk of unauthorized command injection. Predefined command phrases further minimize ambiguity and prevent unintended system activation. The cloud communication layer provides an additional level of security by acting as an intermediary between the user and the embedded hardware. The Sinric Pro platform authenticates incoming requests, manages device identity, and ensures that only validated commands are forwarded to the microcontroller. Secure communication channels are used to transmit data between the cloud and the ESP8266, protecting the system against eavesdropping and data tampering. At the device level, the ESP8266 executes commands only after verifying system state conditions, such as arm/disarm status. This prevents accidental or unauthorized ignition even if a command is received. The use of electrical isolation through a relay module ensures that security breaches at the control level do not directly affect the ignition circuit. Potential threats such as network latency, denial-of-service attacks, and loss of connectivity are mitigated through fail-safe mechanisms. In the event of communication failure or unexpected behavior, the system automatically returns to a safe idle state with the ignition circuit disabled.

VII. EXPERIMENTAL RESULTS



Fig. Hardware prototype showing successful nichrome wire ignition during experimental evaluation.

The proposed voice-controlled rocket launcher was experimentally evaluated under controlled conditions to verify its functionality, reliability, and safety. The experiments focused on validating voice command recognition, cloud communication reliability, system response time, actuator performance, and ignition behavior.

A. Test Setup

The experimental setup consisted of an ESP8266 NodeMCU connected to a servo motor, relay module, and nichrome wire ignition circuit. The system was connected to a Wi-Fi network and integrated with the Sinric Pro cloud platform and Google Assistant. Voice commands were issued from an authorized user account to evaluate end-to-end system performance. All tests were conducted in a controlled environment with appropriate safety precautions.

B. Voice Command Execution

Multiple trials were performed using predefined voice commands such as arming the system and initiating launch. In all test cases, the voice assistant successfully recognized the commands and forwarded them to the cloud platform. The Sinric Pro cloud reliably transmitted the commands to the ESP8266 without packet loss or misinterpretation. No unintended activations were observed during testing.

C. System Response Time

The response time was measured as the interval between issuing a voice command and the corresponding hardware action. Experimental results showed minimal latency, primarily influenced by network conditions. The observed response times were consistent and acceptable for remote ignition applications, demonstrating the feasibility of cloudassisted control for real-time operations.

D. Actuator and Ignition Performance

The servo motor accurately adjusted the launcher orientation as commanded by the controller. The relay-based nichrome wire ignition mechanism operated reliably, generating sufficient heat to initiate ignition within the predefined activation time. Time-restricted relay control prevented overheating of the ignition element and ensured safe operation across repeated trials.

E. System Reliability and Safety

The system demonstrated stable performance over multiple experimental runs. Safety mechanisms such as arm/disarm logic, electrical isolation, and automatic relay shutdown functioned as intended. In the event of network interruption or command failure, the system reverted to a safe idle state with the ignition circuit disabled.

VIII. USE CASE SCENARIOS

This section describes representative use case scenarios that demonstrate the practical applicability, safety benefits, and operational workflow of the proposed voice-controlled rocket launcher. The scenarios focus on controlled environments and

emphasize secure, remote operation. A. Educational Demonstration Scenario

In academic laboratories and educational institutions, the system can be used to demonstrate principles of IoT, cloud computing, embedded systems, and safety-critical automation. An instructor issues voice commands to arm the system, adjust the launcher angle, and initiate ignition from a safe distance. The cloud-assisted validation and device-level safety checks ensure that ignition occurs only under authorized and controlled conditions, reducing risks during demonstrations.

B. Experimental and Prototype Testing Scenario

For experimental rocketry and prototype testing, the system enables researchers to conduct repeated ignition tests without physical proximity to the launcher. Voice commands are used to configure the launcher orientation and trigger ignition remotely. The time-restricted ignition and electrical isolation mechanisms prevent component damage and ensure consistent experimental conditions across multiple trials.

C. Remote Safety Operation Scenario

In environments where direct human access is hazardous, such as outdoor testing areas or restricted zones, the proposed system allows operators to initiate and monitor ignition procedures remotely. The cloud platform ensures secure command transmission, while the embedded controller enforces arm/disarm logic and fail-safe behavior, minimizing the risk of accidental activation.

D. Training and Simulation Scenario

The system can be adapted for training and simulation purposes, where ignition commands are issued without actual fuel ignition or with low-power simulation loads. This scenario enables operators to learn system behavior, command sequencing, and safety procedures without exposure to real hazards, making it suitable for skill development and safety training.

IX. DISCUSSION

A. System Effectiveness

The experimental results indicate that the proposed voice-controlled rocket launcher operates effectively under controlled conditions. The integration of voice commands, cloud-based validation, and embedded control enabled accurate and timely execution of launch-related operations. The system successfully minimized human involvement during ignition, thereby enhancing operational safety. B. Safety and Reliability Considerations

Safety was a primary focus of the system design. The layered architecture ensured that multiple checks were performed before ignition, including voice authentication, cloud validation, and device-level arm/disarm verification. The relay-controlled nichrome wire ignition mechanism provided effective electrical isolation between the low-power controller and the high-current ignition circuit, reducing the risk of hardware damage and unsafe operation.

C. Performance Observations

The system demonstrated consistent response times across multiple test runs. Although minor latency was observed due to network dependency, it remained within acceptable limits for remote ignition applications. The servo motor provided precise launcher orientation, and the ignition mechanism performed reliably with time-restricted activation.

D. Limitations of the Proposed System

Despite its advantages, the system has certain limitations. Dependence on continuous internet connectivity may affect performance in unstable network environments. Relay-based switching, while reliable, may limit long-term durability and switching speed compared to solid-state alternatives. Additionally, the lack of sensor-based feedback restricts real-time monitoring of ignition status and system health.

E. Scope for Improvement

Future enhancements could address these limitations by incorporating solid-state switching devices, sensor-based feedback mechanisms, and offline safety controls. Improving fault tolerance and adding redundancy at the cloud and device levels would further enhance system robustness and reliability.

X. CONCLUSION AND FUTURE WORK

A. Conclusion

This paper presented the design, implementation, and evaluation of a voice-controlled rocket launcher using cloud-based IoT and embedded systems. By integrating Google Assistant, Sinric Pro cloud platform, and an ESP8266 microcontroller, the proposed system enables safe and remote rocket ignition with minimal human involvement. The layered architecture ensures secure command processing, electrical isolation, and controlled actuation, addressing key safety concerns associated with traditional ignition mechanisms. Experimental results demonstrated reliable voice command execution, low-latency cloud communication, and consistent ignition performance under controlled conditions. The relay-controlled nichrome wire ignition mechanism effectively provided electrical isolation and time-restricted heating, enhancing overall system safety. These results confirm the feasibility of applying cloud-assisted voice control to safety-critical embedded applications, particularly in educational and experimental environments.

B. Future Work

Although the proposed system achieves its intended objectives, several enhancements can be explored to improve robustness, security, and functionality. Future work may include replacing the relay-based ignition circuit with a solid-state switching mechanism such as a MOSFET to improve switching speed and durability. The integration of sensors for temperature, current, and ignition status monitoring would enable real-time feedback and system diagnostics. Additional improvements may involve incorporating multi-factor authentication for voice commands, implementing local fallback control to handle network failures, and adding telemetry and data logging capabilities for

performance analysis. The system can also be extended with camera-based monitoring and mobile application support to provide enhanced situational awareness. These enhancements would enable the proposed architecture to be adapted for more advanced research and training applications.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to **Ms. Seema C K**, Assistant Professor, Department of Computer Science and Engineering(*IoT, Cyber Security including Blockchain Technology*), Maharaja Institute of Technology Mysore, for her valuable guidance and continuous support throughout the course of this project. Her insights into Internet of Things (IoT) architectures, cloud-based automation, and embedded system design were instrumental in shaping the technical direction of our work.

REFERENCES

- [1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
- [2] L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.
- [3] Google LLC, "Google Assistant Developer Documentation," [Online]. Available: <https://developers.google.com/assistant>
- [4] Sinric Pro, "Sinric Pro Cloud Platform Documentation," [Online]. Available: <https://sinric.pro>
- [5] Espressif Systems, "ESP8266 Technical Reference Manual," Espressif Systems, 2023.
- [6] S. Monk, *Programming Arduino: Getting Started with Sketches*, 2nd ed., McGraw-Hill Education, 2016.
- [7] R. Kamal, *Embedded Systems: Architecture, Programming and Design*, 3rd ed., McGraw-Hill Education, 2015.
- [8] K. Ashton, "That 'Internet of Things' Thing," *RFID Journal*, 2009.
- [9] M. Collotta and G. Pau, "A Novel Energy Management Approach for Smart Homes Using Bluetooth Low Energy," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 12, pp. 2988–2996, 2015.
- [10] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, "Convergence of MANET and WSN in IoT Urban Scenarios," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3558–3567, 2013.
- [11] M. Ammar et al., "Internet of Things: A Survey on the Security of IoT Frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.
- [12] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
- [13] IEEE Standards Association, "IEEE Standard for IoT Architecture," IEEE, 2020.
- [14] A. Zanella et al., "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.
- [15] B. Rashidi and C. Fung, "A Survey of Algorithms and Control Techniques for Energy Management of Smart Buildings," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2087–2100, 2016.