International Journal of Engineering Research and Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 22, Issue 4 (April 2026), PP 153-156

Smart Access Security System with IoT Integration Simulation in NI LabVIEW

[1.]Mansi Jonwal, [2.]Shreya Kharade

[1] *Department of instrumentation engineering AISSMS IOIT*
[2]*Department of instrumentation engineering AISSMS IOIT*
Pune ,Maharashtra, India

ABSTRACT
This paper presents the design and implementation of an automated security system simulated using NI LabVIEW. The system bridges the gap between local hardware control and cloud-based mobile notifications by integrating a digital keypad for authentication with a live camera feed for continuous monitoring. Using state-machine logic, machine vision, and secure HTTP web communication, the platform provides a highly responsive approach to automated building security.

Date of Submission: 28-03-2026 Date of acceptance: 08-04-2026

I. INTRODUCTION

In today's connected world, real-time monitoring is essential for protecting physical spaces. This simulated project introduces an IoT-enabled doorway/security authentication simulation for access control. The system validates user credentials/saved password and provides real-time intruder alerts via Telegram Bot alongside local visual feedback. This system works like a smart lock, access system helping the user to have smart monitoring and security for areas they want to protect.

The system has a camera, a keypad and a Module for alert notification. (here a telegram bot is used). The keypad is the input the user enters the password and the system has a simple logic of checking if the entered password matches the saved password in the memory i.e. the correct password. If it matches the door unlocks. But if it doesn't then a series of case statements are triggered that result in image capturing and alert sending.

II. SYSTEM ARCHITECTURE

The system is built on a State-Machine-inspired While Loop architecture and multiple case statements:

1. **Idle State**: The system remains inactive until the "Submit" trigger is pressed; the submit button here is also set to latch on release .
2. **Authentication State**: A string comparison algorithm validates user input against a predefined master key or the predefined password, "1234".
3. **Success Protocol**: If the password matches, a "Door Status" LED lights up/ glows, and the system resets for the next user or for next password input once the door is locked or closed.

Security Protocol: If an unauthorized attempt or wrong password is detected or read, a multi-layered response is initiated, including image capturing and remote notification

III. METHODOLOGY

The system follows a structured approach to transition from local hardware input to cloud-based alert generation:

1. **Initialization**: At startup, the system initializes hardware sessions for the camera (cam0 ; here local webcam) and the HTTP client.
2. **Wait State (Idle)**: The program enters a main While Loop that waits for the user to interact with the digital keypad once the user types the password the system reads after it is submitted.
3. **Authentication Logic**: When the "Submit" button is pressed, the system performs a string comparison between the user's input and the master key that is already saved inside, the original main password is already saved in a string constant in the equal comparisons one input the other input is from the password display the one the user types.
4. **Decision Branching**: If the password is correct, the door LED turns on; if incorrect, the security protocol triggers that is the case structure of image capturing and alert notification works.
5. **System Termination**: The loop works once the image is captured an alert pop up displays and the alert is sent through bot. After this the system waits for the next password input, if the correct password is entered then the door led turns on if not the same image capturing and alert block works.

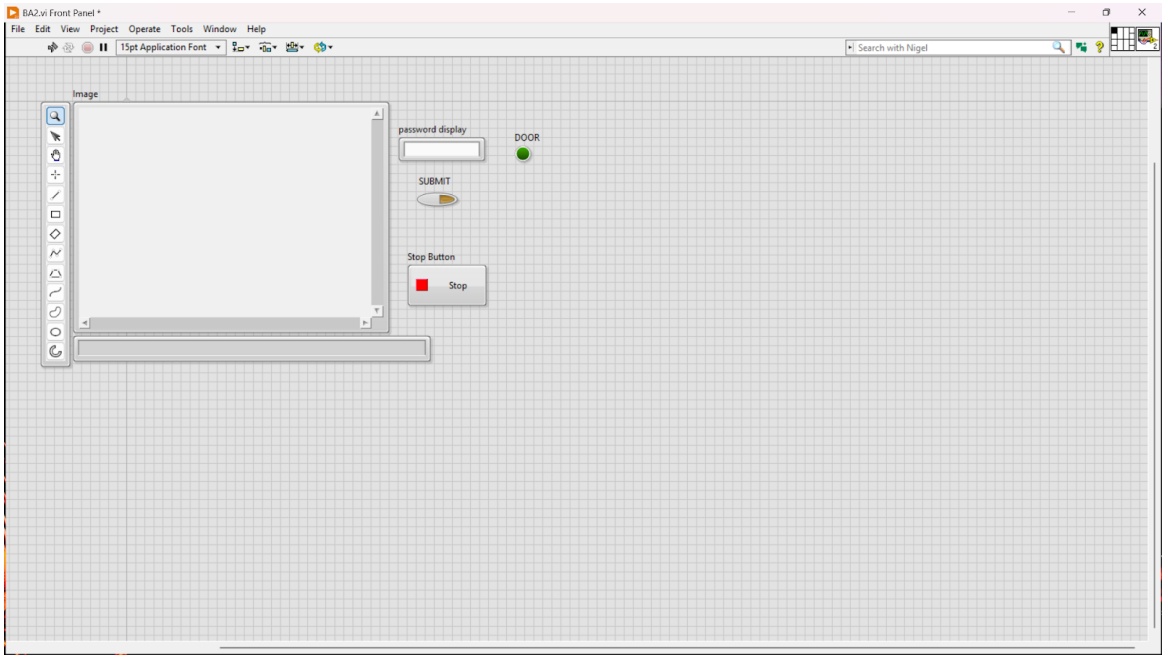

FIGURE 1. Front panel

IV. BLOCK DIAGRAM

The LabVIEW block diagram defines the graphical source code and logic execution:

1. **Case Structure**: This is used to handle the "True" (Success) and "False" (Failure) conditions of the password validation.
2. **Vision Acquisition using (IMAQdx)**: The IMAQdx Snap VI is specifically wired to the "False" case of the logic so the false case of the password recognition powers only when the wrong password is entered and this starts the next logic of image capturing. It captures a frame from the live video buffer only when the wrong password is detected.
3. **IoT and HTTP Integration**: The diagram features an HTTP GET function. Logic within the diagram dynamically builds a URL string containing the Bot API Token and Chat ID.

4. **Protocol Handling**: To prevent SSL/TLS errors (Error 363507), the "Verify Server" attribute is programmatically set to False within the diagram.
5. **Shutdown Logic**: A three-input OR Gate monitors the manual Stop Button, the confirmation that the Telegram message was sent, and the user's acknowledgment of the alert dialog. So the system won't stay constantly in loop.

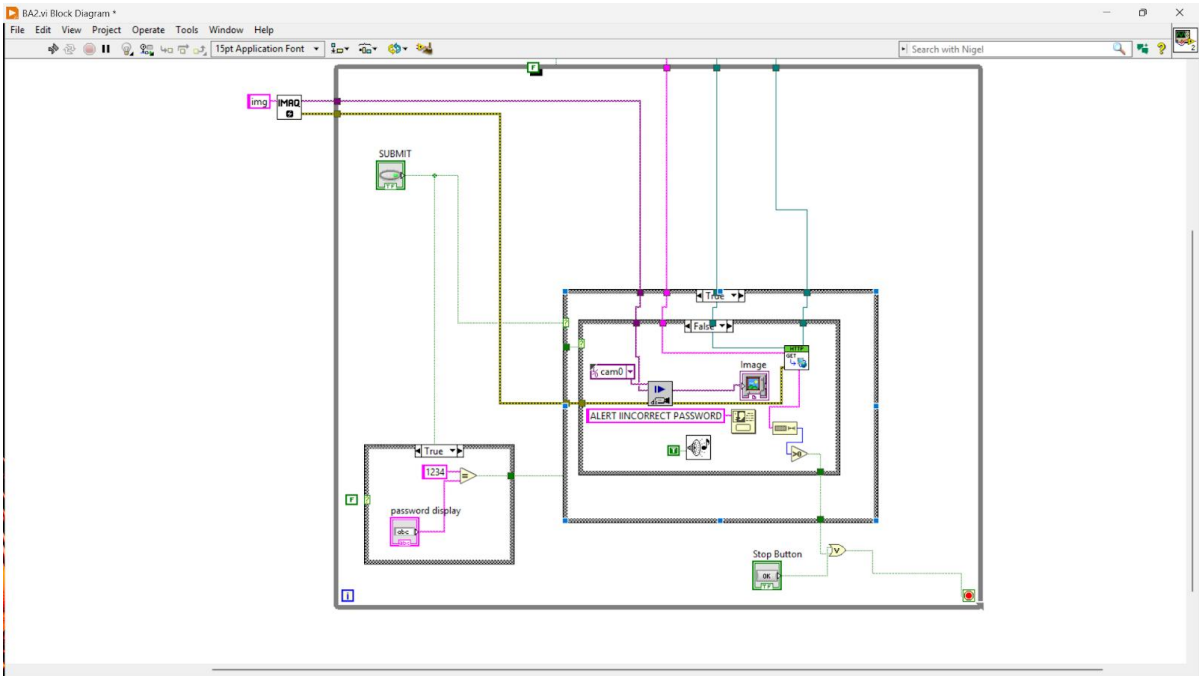

FIGURE 2. Block diagram of the system

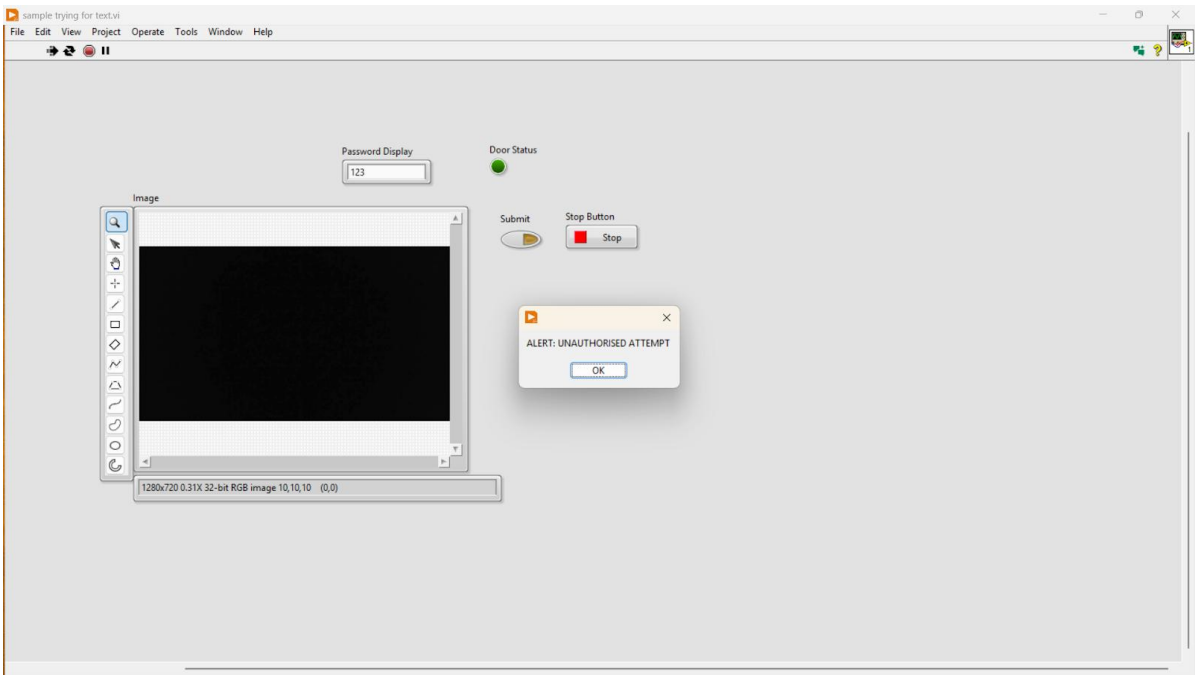

FIGURE 3. Front panel output (alert pop up)

V. DISCUSSION AND CONCLUSION

The system successfully demonstrated a dual-layer alert mechanism:

- The image of the intruder is captured and displayed on the front panel.
- The project successfully integrates hardware control and modern IoT protocols, providing a scalable foundation for advanced security environments. The owner or the verified authorized personnel receive the alert on their mobiles where they have the text synced.

REFERENCES

[1]. "IoT Based Human Intrusion Detection System using Lab View," *ResearchGate*, Aug. 2025.
[2]. **S. Tippannavar**, "Smart Home Automation Implemented using LabVIEW and Arduino," *ResearchGate*, Sept. 2022.
[3]. **Researcher**, "Low-Cost Home Security Notification System Using IoT and Telegram Bot," *Journal of Computing Research and Innovation*, Dec. 2025.
[4]. **Kumar**, "Design and Implementation of an IOT Enabled Classified Authentication System using LabVIEW," *IJRASET*, Apr. 2023.