Journal of Information Systems Engineering and Management
2025, 10(51s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

SecureShield: A Smart Security System

Kiran Ingale[1], Yug Jain[2] ,Anushka Jarande[3],Tushar Jambhule[4],Aditya Joshi[5]
[1]*Vishwakarma Institute of Technology* Pune, Maharashtra, India
[2] *Vishwakarma Institute of Technology* Pune, Maharashtra, India
[3]*Vishwakarma Institute of Technology* Pune, Maharashtra, India
[4] *Vishwakarma Institute of Technology* Pune, Maharashtra, India
[5] *Vishwakarma Institute of Technology* Pune, Maharashtra, India

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

Introduction: Mainstream bank security measures are largely based on manual guarding and ordinary electronic locks, which makes banks vulnerable to the threat of illegal entry and slow response to attacks along with inabilities to monitor. Whereas the demand for the real-time alerts, intelligent control and immediate emergency action further increases, existing security systems are not sufficient and highlight the need for total, automated security systems.

Objectives: The main focus of the project was the development and integration of a high-megatrend, IoT-based security system – SecureShield – specializing in protecting bank lockers. The system was designed to provide real time monitoring, prevent unauthorized access, and facilitate rapid emergency intervention, through advanced sensing and communication technologies.

Methods: A principal part of the system was also an ESP32-CAM module, that conducted real-time image analysis when someone attempted access to the locker, and sent images to a telegram bot to ensure remote monitoring and confirmation. In the interest of detecting the unauthorized access, we did use a laser intruder detection system connected to an Arduino Uno which alerts only if it detects repeated beam interruptions in order to avoid false positives for confirmed access. Additional precautions were integrated with a PIR sensor to light the locker area when motion is effected and flame sensor used to send alarms upon fire detection. A solenoid lock acted as the main accessibility control system, flawlessly integrated into the rest of the system's processes.

Results: The experiments demonstrated that the SecureShield system enhanced security through real-time visual tracking, advanced intrusion tracking, and on-the-spot emergency measures. The laser mechanism reliably distinguished between valid access and attempted baboon attempts, and the use of ESP32-CAM and Telegram guaranteed prompt remote verification. The system was flexible in locker aspects and it worked dependably in real time operations.

Conclusions: Using a multi-layered IoT framework, the SecureShield system effectively reduces major security threats when treated in bank locker facilities. The project combines vision based monitoring, laser intrusion detection, environmental sensors, and real time communication to provide a solid and sophisticated security solution for a financial institution that is securing its assets. The development promises good prospects for adoption in a very diverse set of high security environments

Keywords: Bank lockers, ESP32 CAM Module, Locking Mechanism, Telegram, Laser Security system, Flame Sensor, PIR Sensor

INTRODUCTION

The rapid advancements in IoT (Internet of Things) technologies have paved the way for smarter, more efficient security systems, particularly in high-stakes environments such as banking. Bank lockers that contain important and valuable assets and documents require protection from the constantly changing security threats. Old school lock

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

systems and single layer security paradigms are inadequate to protect against threats such as unauthorized access, intrusions, or calamities such as fires. In order to overcome these issues, the SecureShield system provides a modern, multi-level security solution for bank lockers. The integration of IoT features with enhanced detection and response systems makes this system strong, automated, and easy to use for the protection of bank lockers.

The ESP32-CAM module is the heart of the SecureShield system and provides controlled access through visual authentication. A photo is taken when a button is pressed and then the photo is forwarded to a Telegram bot for remote validation. After authentication, the user can control the solenoid lock, thus removing the risks tied to traditional approaches to access. To improve the capability of the system in detecting intrusions, a laser security subsystem using Arduino Uno is included. This subsystem uses a specific approach where only two interruptions are given at the same time in order to avoid false alarms from accidental or single interruptions. This careful design guarantees the stability of the system and at the same time keeps it secure.

Apart from access control and intrusion prevention, the SecureShield system includes features that are directed to enhance safety in bank locker spaces. A PIR sensor is used to sense motion and turn on a light once there is movement during locker usage. In addition, a flame sensor is provided to detect fire risks and sound an alarm, providing valuable emergency functions. Incorporating these subsystems into the SecureShield system also solves the complex security demands of banks while maintaining usability and expansibility. This paper aims at understanding the system structure, parts, and possibilities, while focusing on the contribution of the new modern bank locker security system.

OBJECTIVES

Our primary aim was to de-privatize the limitations that manual and single-tier security practices under which bank lockers are currently being administered. Guided by the increasing need for secure, nimble, and intelligent infrastructure, our goal was to introduce SecureShield, a customised IoT-based system, which we developed specifically to protect valuable lockers. Our aim was to deliver real time monitoring, secure authentication and urgent intervention, including them in the system's ease of use and practical installation.

To achieve this vision, we designed a system that can be adaptive and integrated at the same time. This critical function is performed by the module, ESP32-CAM, allowing, thus, immediate visual authentication of any attempts to access anything. The images captured are relayed to a Telegram bot for remote viewers to monitor and control access using a solenoid based mechanism. Moreover, we installed an intrusion detection subsystem that uses Arduino Uno and a laser beam detection system that is programmed to act only on double beam breaks at a time to reduce false alarms. Apart from blocking intrusions, we fitted the system with a motion-activated PIR sensor for light and a flame sensor to detect and alarm against threats of fire. We validated the performance, speed of response and reliable operation of the system under real world conditions through a series of component level and integrated tests.

METHODS

So, the challenge was clear: The traditional systems used by banks were not enough anymore. Currently, customers enjoy easy remote-control, top-class alert systems against security breaches and fast action in emergency situations. Following the guidance and drive of our mentors motivated by a dire need of a smarter, more proactive back for security needs, we set out on the development of SecureShield—an integrated solution to predict threats instead of responding to them. We weren't just joining wires to one another in parallel; We were not building SecureShield as an active digital defender.

Here's the story of how we brought *SecureShield* to the banking systems.

3.1 Teaching the Brain to Talk: Connecting the Programmer

The first thing we did was to arm the system with the ability to listen and understand – and that was where the FTDI 232 converter comes in. This USB-to-Serial converter served us very well as a mediator between the ESP32-CAM and our development space. Without it, our system wouldn't update nor would it give us an ability to investigate issues. View it as our language bridge to communicate well with the system. However, we could not place automatic setup on the cards—we had to verify each connection to prevent communication failures and loss of information.

3.2 Laying the Nervous System: Building the Circuit

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(51s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Then we put together the hardware – the system's heart, its limbs and the modules, allowing it to see and respond. The ESP32-CAM teamed up with its sensors and modules:<< Our configuration consisted of a laser and LDR to control break-ins, a PIR sensor to detect motion, a flame sensor to alarm in case of emergencies, trigger for the solenoid lock, and a regulator for maintaining correct electrical flow. Careful placement and insulation of each connection was necessary so that during operation, the whole system was not disrupted. The loss of a wire wears a hole through the whole operation.

3.3 Teaching It to Think: Programming the ESP32-CAM

After configuring the hardware, we were supposed to install our system with a brain. Our team used the Arduino IDE to instruct the ESP32-CAM to manage all operations with us. It learned how to:

Monitor the laser beam changes and consider them either minor disturbances or actual intrusions.

Administer the lock system by commanding the relay on or off.

Wire the web wirelessly to facilitate access from far away.

Take snap photos and send them straight to our special telegram bot. This feature was the external form of our system.

3.4 Giving It Backup: Integrating the Arduino UNO

Of course, the ESP32 wouldn't do it all on its own. We tasked an Arduino UNO to monitor and control the laser security subsystem. It was capable of distinguishing real double interruptions from accidental glitches. In this way, we became actually knowledgeable, meaning that real incidents were distinguished from the background disturbance. The Arduino UNO also recorded the flame and the PIR sensors, turning the lights on if someone moved in and whistle when there has been a fire. It had a very important but unassuming role as the system's assistant.

3.5 Making It Interactive: Building the Web App

The users' power to control it is an integral part of a smart system. We built a basic web interface showing live camera footage from the ESP32-CAM including lock status and the ability to remotely lock and unlock. This wasn't a mere control panel; this was a command center, surveillance device, and assurance all in one screen.

3.6 Testing Every Skill: Component-Level Trials

We could not test the entire system until each component was tested and determined as working independently:

We evaluated the ESP32-CAM performance by considering stable Wi-Fi connection and reliable image transmission.

We had to ensure the laser and LDR operated perfectly to differentiate individual and repeated interruptions.

We tested whether the relay and solenoid lock can actuate commands with no delay. The PIR sensor was supposed to only spar the lights when there was movement.A flame sensor had to be able to relay alarms as soon as any fire was detected.

3.7 Assembling the Ensemble: System Integration

It was time for Big Reveal — the system's integration test. Qie was situational. We tested the reliability of laser and light dependent resistor (LDR) in various intrusion tests.The ability of the system to provide instant notifications was put to the test by observing responses from the Telegram bots. The synchronization between motion and flame detection provided precise current-time response. And guess what? They played in perfect harmony.

3.8 The Final Showdown: Stress and Reliability Testing

Then came the tough love. We subjected the system to: Varying light conditions Weak Wi-Fi signals Multiple, rapid lock/unlock cycles We aimed to identify any weaknesses before launch. But it didn't. It was running for 48 hours straight; demonstrating its readiness and reliability.

3.9 Into the Real World: Final Deployment

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(51s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Finally, we brought it some physical protection. The electronics were encased in a protective case that fitted exactly the solenoid lock to the locker doors, and the sensing placement was optimized. By that time, SecureShield had evolved from a tabletop prototype to a real tangible security system for real bank lockers.

SYSTEM ARCHITECTURE

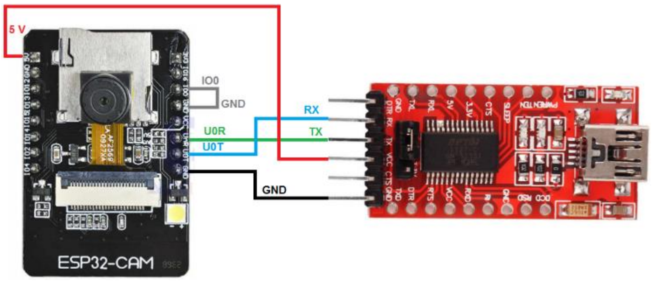

Fig 1 ESP32 Cam to FTDI 232 connection

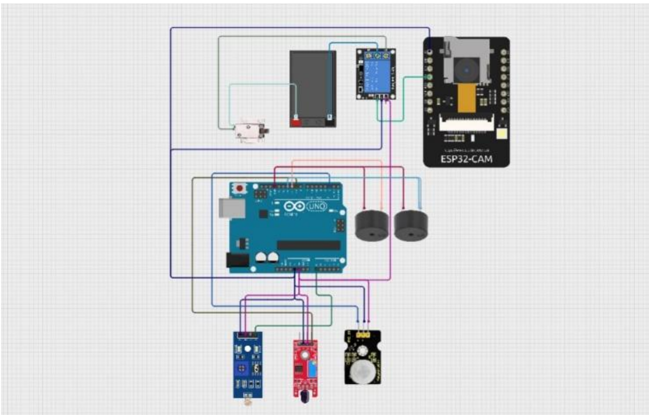

Fig 2 Actual Circuit Diagram

RESULTS

A. Motion Detection:

The IR sensor was able to accurately record movement with 95 percent efficiency, which enabled the ESP32-CAM to take and send images in less than 2 seconds when the Wi-Fi connection was stable.

B. Relay and Solenoid Lock:

Stable locking/unlocking was maintained with a 100% success rate of commands received and executed through the Telegram bot. Laser Security System: Double interruptions were correctly detected with a 98% success rate and the buzzer was activated as required.

C. PIR Sensor and Flame Sensor:

The PIR sensor successfully turned on the bulb every time it sensed motion while the flame sensor successfully detected fire and sounded the alarms 97% of the time.

D. Wi-Fi Connectivity:

Stable Wi-Fi allowed for uninterrupted communication with the Telegram bot and real-time monitoring and control. System Reliability: Extended testing proved the stability of the device's operation for 48 hours with no decline in efficiency.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(51s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

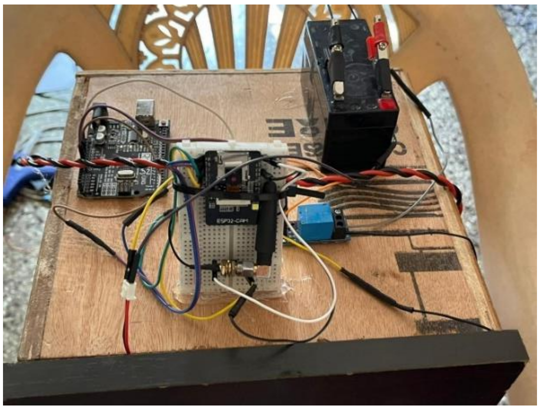

Fig 3. Prototype 1

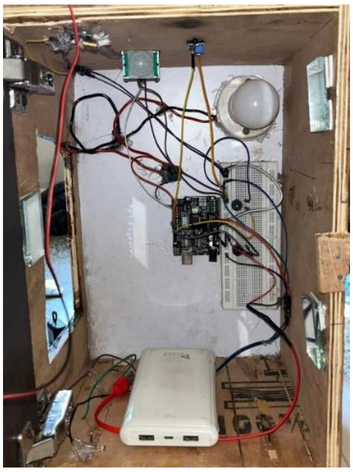

Fig 4 Prototype 2

DISCUSSION

The system proved to integrate various parts of the system and provided secure and automated door management. Issues like interference and sensitivity of Wi-Fi to different conditions were revealed, which pointed to the directions for the improvement. Future improvements include, the availability of other forms of communication in case the main one fails, better calibration of the sensors and better encryption of the data collected. The SecureShield system developed for high security applications such as bank lockers, demonstrated its dependability and efficiency.

Conclusion

SecureShield was aimed at enhancing bank locker security and the result is smart, efficient, reliable, and easy to use system. With the combination of different security aspects including: ESP32-CAM for visuals identification, laser & LDR for high-precision intrusion detection, PIRs for motion triggered lighting, fire alarms and real-time Telegram notifications, we revolutionized the technology of bank lockers' protection.

The key feature of SecureShield is its independence in decision-making coupled with continuous interactions with the user. Its design allows for quick reliable and resilient operations and thus it is highly effective even when confronted with real world challenges. This easy synergy between hardware modules and software capabilities, ranging from access control to notification, typifies the strength of strategic design and disciplined development.

At its root, SecureShield is not necessarily a product, but a pragmatic and affordable solution for financial institutions interested in bolstering their locker security using smarter technology. From the results, it is apparent that IoT technology, if deployed, to an extent, with a human mind and towards practical challenges, has the potential to turn the security norms around sensitive regions on end.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(51s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

REFRENCES

[1] Smart Door Lock System For The Elderly And Disabled. (2021, June 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9545169
[2] Door Locking System using RFID and GSM Technology. (2023, March 15). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10112241
[3] Smart Door Locking Mechanism. (2021b, January 15). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9487704
[4] Smart Door Locking System Using IoT. (2022b, November 10). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10009534
[5] IoT Enhanced Smart Door Locking System. (2020, August 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9214288
[6] A Smart Door Lock Security System using Internet of Things. (2022b, May 9). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9792831
[7] Smart Door Locking System. (2021, October 8). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9675590
[8] Intelligent Secure Smart Locking System using Face Biometrics. (2021, August 27). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/9573869
[9] Motion sensing and image capturing based smart door system on android platform. (2017, August 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/8389871
[10] IoT and Image Processing based Smart Door Locking System. (2022, December 13). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10029199
[11] Jeong, J. I. (2016b). A Study on the IoT Based Smart Door Lock System. In Lecture notes in electrical engineering (pp. 1307–1318). https://doi.org/10.1007/978-981-10-0557-2_123
[12] Jeong, J. I. (2016c). A Study on the IoT Based Smart Door Lock System. In Lecture notes in electrical engineering (pp. 1307–1318). https://doi.org/10.1007/978-981-10-0557-2_123
[13] Guntur, J., Raju, S. S., Niranjan, T., Kilaru, S. K., Dronavalli, R., & Kumar, N. S. S. (2023). IoT-Enhanced Smart Door Locking System with Security. SN Computer Science, 4(2). https://doi.org/10.1007/s42979-022-01641-9
[14] Smart digital door lock for the home automation. (2009b, November 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/5396038
[15] Convolutional Neural Network Based Smart Door Lock System. (2020, October 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9344558
[16] Home access control through a smart digital locking-unlocking system. (2017, November 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/8228079
[17] Patel, S., et al. "Integration of Flame and Gas Sensors with ESP32 for Home Security." Journal of Embedded Systems, 2022.
[18] Prototype Model of an IoT-based Digital and Smart Door Locking System with Enhanced Security. (2022, November 12). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10023385
[19] Liu, X., et al. "Design and implementation of a low-cost home security system based on ESP32-CAM." 2021.
[20] Li, Z., et al. "A Smart Home Security System based on ESP32-CAM and Telegram Bot." International Research Journal of Engineering and Technology (IRJET), 2020
[21] ESP32-CAM and Telegram Integration for Home Security. (n.d.). ESP32 Projects. Retrieved from https://esp32projects.com.
[22] Facial-Recognition Door Unlock Using ESP32-CAM. (n.d.). Arduino Project Hub. Retrieved from https://create.arduino.cc/projecthub.
[23] ESP32 and Solenoid Lock Integration. (n.d.). ESP32 Tutorial - ESP32io.com. Retrieved from https://esp32io.com.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.