Industrial Engineering Journal
ISSN: 0970-2555
Volume : 55, Issue 01, No.1, January : 2026

A SECURITY SYSTEM FOR A CUPBOARD USING THE ESP32 AND ESP32-CAM MODULE WITH A KEYPAD AND FINGERPRINT UNLOCK SYSTEM

Mr. Amey H. Wani, Mr. Parth C. Gurav, Mr. Anurag S. Gupta, Mr. Sahil D. Sarang, Student, Dept. Of Electronics and Telecommunication Engg., Vishwakarma Institute of Technology.
Mrs.A.Sreelatha, Assistant Professor, Dept. of Computer Science, University Arts and Science, College, Kakatiya University.
Dr P. Praveen, Associate Professor, Dept. Of CS&AI, SR University.

ABSTRACT
Modern security systems are widely used to protect valuable items such as jewelry, documents, and confidential materials. However, many existing solutions still suffer from security gaps. This paper proposes an improved IoT-based cupboard security system that offers multi-layer protection and high reliability. The system uses an ESP32 as the main controller and an ESP32-CAM as a secondary controller for image-based evidence collection. It integrates a 4×4 matrix keypad and a biometric fingerprint sensor for dual factor authentication, an LCD for user interaction, a GSM 2G module for real time alerts, a vibration sensor for detecting forced entry attempts, and a solenoid lock for secure physical locking. In case of intrusion or abnormal vibration, the system notifies the owner via GSM and captures photographic evidence using the ESP32-CAM, enhancing post-incident verification. Overall, the proposed system addresses key gaps in traditional cupboard security methods and provides a more reliable and robust protection solution

Keywords: IoT, Security system, Microcontrollers, GSM module, Fingerprint unlock

I. Introduction
Security has always been a fundamental priority for individuals and societies alike. With the increasing value of personal assets and the sophistication of criminal activities, the need for reliable and intelligent security systems has become more pressing than ever. For instance, the average global loss due to jewellery robbery is estimated at around 1.2 billion USD, with a recovery rate of only 2% [1]. In India, according to the National Crime Record Bureau (NCRB), the total value of robberies amounts to nearly 830 billion USD, with a recovery rate of approximately 29.2% [2].

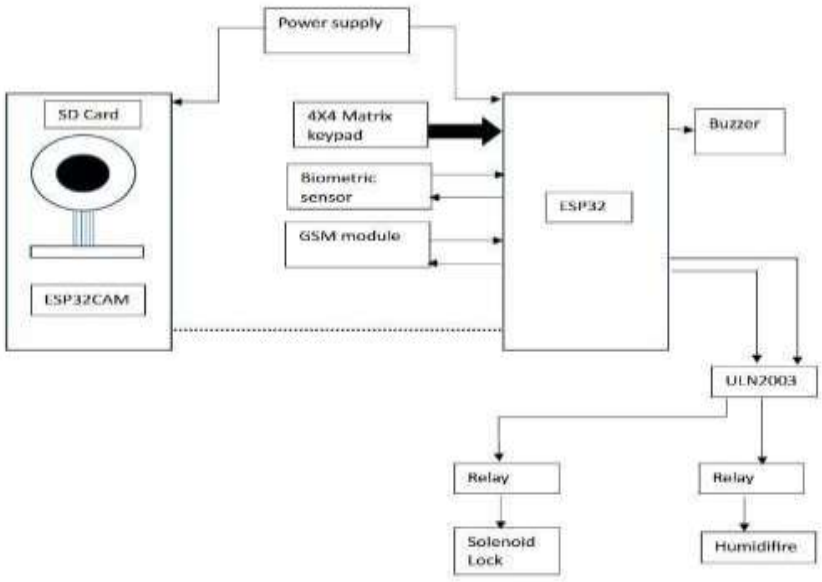

Fig. 1: Block diagram

These statistics underscore the urgent requirement for advanced, proactive, and highly responsive security solutions. In recent years, Internet of Things (IoT) technology has revolutionized the way security systems are designed and implemented [3]. IoT enables seamless integration of sensors, communication modules, and intelligent algorithms to create systems that are not only preventive but also responsive to threats in real time. Existing IoT-based security solutions, however, often remain limited in scope. For example, one system discussed in prior research focuses primarily on Alzheimer's patients, offering basic protection through fingerprint authentication and a buzzer alarm [4]. While useful in specific contexts, such systems lack the versatility and robustness required to counteract broader threats such as burglary or unauthorized access to valuable storage units. To address these limitations, the system proposed in this paper introduces a multi-layered cupboard security solution that combines authentication, detection, and counteraction mechanisms. Unlike conventional designs, this system employs dual authentication methods a password and fingerprint recognition to ensure that only authorized users gain access [5]. Beyond authentication, it integrates vibration sensors capable of detecting unnatural or forced movements, such as attempts to break open a cupboard door [6]. Upon detection of such activity, the system activates a GSM module that immediately alerts the owner via a phone call, while simultaneously triggering a buzzer alarm to deter intruders [7]. This dual response mechanism not only informs the rightful owner but also creates an immediate deterrent effect. The novelty of this system lies in its comprehensive counteraction strategy. While existing cupboard or storage security systems typically focus on single-layer protection, the proposed design combines preventive authentication, real-time detection, and active deterrence [8]. Such an integrated approach ensures that unauthorized access attempts are not only blocked but also actively countered, thereby significantly reducing the likelihood of successful theft. To the best of our knowledge, no comparable cupboard-specific security system currently exists in the market that offers this level of layered protection and responsiveness [9]. By leveraging IoT technologies and combining them with practical hardware modules, this system represents a new paradigm in personal asset security [10]. It is designed to be affordable, scalable, and adaptable to different environments, making it suitable for households, offices, and institutions where safeguarding valuables is essential. Ultimately, this work contributes to the growing field of IoT-based security by presenting a solution that is both innovative and highly practical, bridging the gap between theoretical research and real-world application [11].

II. Literature

The need for enhanced security mechanisms has been emphasized, and a system integrating both keypad-based authentication and fingerprint-based access control has been proposed to improve reliability and user authentication.[12] A security system incorporating fingerprint-based access control and magnetic sensors for detecting door opening and closing has been presented. However, the system does not include mechanisms for capturing evidence during a robbery or for detecting abnormal vibration conditions.[13] A security system utilizing a keypad and RFID tags for access control has been proposed; however, no response or action is defined in the event of a robbery.[14] A web-based home security system has been developed to provide comprehensive protection, with an ESP32-CAM module integrated for surveillance. However, the system is designed for overall household security and does not specifically address cupboard-level protection. [15] The system is designed specifically for Alzheimer's patients to assist with daily activity tracking by recording the number of times a door is opened. Since it does not incorporate any security or access-control features, it is suitable only for storing items such as medicines or clothes and cannot be classified as a security system.[16] A voice-controlled home automation system has been implemented in which door access is achieved using a keypad and voice commands, with password modification enabled

through voice input. An Arduino microcontroller is used to process and interpret the voice commands; however, the system is intended for room-level doors and general home automation rather than cupboard-specific security.[17]

2.1 Methodology

Case 1: To open the door of the cupboard:

The user must enter the correct 6-digit password. There will be three attempts to enter the correct password. If the entered password matches the correct one, the solenoid lock will trigger and open the cupboard door [18].

If the entered password is incorrect, a message will display on the LCD, giving a second chance to enter the password. If it matches, the door will open. If the password is wrong again, a message will appear on the screen prompting the user to try fingerprint authentication as a secondary option, with three attempts. If the fingerprint enrolled by the user matches within three tries, the door will open; otherwise, the security system will reset [19].

The process in the security system:

The solenoid lock will not change its state. The buzzer will start ringing. The camera from ESP32CAM will start taking pictures with a duration of 5 seconds and store them in the memory card. Simultaneously, make an alert call to the main user using the GSM module. And then after 5 minutes, the system will again get ready to accept the passwords and fingerprint.[20]

Case 2: If an unauthorized person attempts to open the case without using the password or enrolling their fingerprint, and accesses it by damaging the cupboard or hitting it, then the vibration sensor will detect unnatural vibration and trigger the same security practices discussed above [21].

Case 3: Reset the system

If the main user opens the door correctly, the security system will be deactivated as long as the door remains open. Once the user finishes his/her work and closes the door, the system will reset. This is done by the door switch connected near the door. In case of forced entry, the security system will turn on, and if the user is satisfied with the security process, He/she will re-enter the correct password or enroll the fingerprint and can reset the system [22].

2.2 Component Description

1. ESP32: We used ESP32 as the main microcontroller to manage most of the tasks. It facilitates a dual-core 32-bit LX6 microprocessor ,2.4GHz Wi-Fi (802.11b/g/n), and Bluetooth connectivity. It uses memory of 520Kb and 4Mb flash memory.

2. ESP32CAM: This controller is a co-controller for this project. It consists of a camera module that is responsible for taking photos of the threat situation. The controller also consists of an SD card slot. In addition to that, it has 802.11b/g/n Wi-Fi and a Bluetooth 4.2 module.

3. FPM10A fingerprint sensor: The biometric sensor used for user identification. The technical features of FPM10 are: It operates on 3.6v, it can store up to 200 fingerprints, The Fase Accept Rate is less than 0.001%, the False Rejection Rate is less than 1.0%, search time is around 1 sec.

4. Vibration sensor: we used a vibration sensor SW420 module, which operates on on 3.3V, It gives a digital output in the presence or absence of significant vibration. It consists of a comparator chip LM393, which compares the sensed vibration with a set threshold.

5. GSM: This is used to make the alert call to the user. The name of this module is SIM900A GSM module. It supports 2G communication, uses dual bands of 900 MHz and 1800 MHz. The communication protocol used is UART, and it operates on a 4.5V DC supply. In addition to that, it uses an SMA connector for an external GSM antenna and Audio Interface.

2.3 Results and discussion

The above image shows the working model of the proposed system. The user opens the door by entering the correct password. He also has another option of enrolling in a fingerprinting. The system was working as described in the methodology. It was properly responding for threats and saving the picture in the memory card in the ESP32CAM [23]. If we talk about the disadvantage of the current system, the system fails when the power supply is cut off. But this problem can be resolved by using a battery backup [24].

Fig. 2: Working model of the proposed system

2.4 Future Scope

The system addresses most of the gaps in the existing system, such as relying solely on a password or fingerprint for authentication. If the system provides both, it does not include a mechanism to detect unnatural vibrations, and most importantly, none of the systems keep a record of incidents.
The system I have proposed requires some updates. Currently, the system cannot be accessed remotely, so I plan to build an app or website to indicate:

1. Status of the door.
2. The number of times the door is opened.
3. Who has opened the door if it is through a figure print
4. The system can be reset through the website or app instead of re-entering the password.
5. Upload the photos taken during the threat to the website.

These ideas are proposed to give software support to the system. If we talk about the hardware updation the my plan is

1. Provide a button that will help to switch from password to fingerprint and vice versa.
2. Add a 4G GSM module.
3. Use Raspberry Pi instead of ESP32 .
4. Provide battery backup in case of a power failure.

This improvement will make the system fully protected from threats. And no other requirement is needed for this kind of system. The cost of the system will increase by 15% from the baseline (baseline is around 5000 INR) [25]. But it will be completely worth it. This kind of updation is really

required in order to protect our precious things from robbery. So the scaling of the system will be more profitable, and it can be the market-leading product [26].

III. Conclusion

So the System is protected in multiple directions and hence very useful for businessmen like jewelry shops, industrialists, CAs, CEOs, Defences, Ministries, etc. As this kind of environment has very confidential information so the priority of security is always at the top. The system is very dynamic, and it can be modified as per the user's requirements. It is backed by IoT technology, and it is an integration of both software and hardware. For the proposed system, ESP32 works as the main microcontroller and works efficiently and quickly. The GSM module facilitates real-time communication. And the unique part of this system that makes it different from other systems is the use of a vibration sensor and a camera. Now talking about the locking system, it uses a strong solenoid lock which operates on 12V. Overall system provides a high level of security and automation; the only minus point is that it is costly. But is the cost of this product worth it.

References

[1] I. García-Magariño, F. González-Landero, R. Amariglio, and J. Lloret, "Collaboration of Smart IoT Devices Exemplified With Smart Cupboards," IEEE Xplore, Jan. 1, 2019.
[2] M. M. Nasralla, I. García-Magariño, and J. Lloret, "Defenses Against Perception-Layer Attacks on IoT Smart Furniture for Impaired People," IEEE Xplore, 2020.
[3] N. N. S. Hlaing, "Electronic Door Lock using RFID and Password Based on Arduino," Int. J. of Trend in Scientific Research and Development (IJTSRD), Mar.–Apr. 2019.
[4] N. Rahma, "Development of a Fingerprint-Based Door Lock System Integrated with a Security Camera System," Pinisi J. of Science and Technology, Jan. 31, 2024.
[5] F. González-Landero, I. García-Magariño, R. Amariglio, and R. Lacuesta, "Smart Cupboard for Assessing Memory in Home Environment," [Journal/Publisher not specified.
[6] R. D. H. Arifin, "Door Automation System Based on Speech Command and PIN using Android Smartphone," Proc. Int. Conf., IEEE Xplore, 2018.
[7] D. Hercog, T. Lerher, M. Trunti˘c, and O. Težak, "Design and Implementation of ESP32-Based IoT Devices," MDPI, 2023.
[8] P. W. Rusimamto, Endryansyah, L. Anifah, R. Harimurti, and Y. Anistyasari, "Implementation of Arduino Pro Mini and ESP32-CAM for Temperature Monitoring on Automatic Thermogun IoT-Based," Indonesian J. of Electrical Engineering and Computer Science, Sept. 3, 2021.
[9] M. D. SAS, "Intelligent Fingerprint-Based Access System with Camera," Carpathian J. of Electrical Engineering, vol. 1, 2021.
[10] [10] I. E. A. Pakpahan, P. Sihombing, and M. K. M. Nasution, "Analysis of the SW-420 Vibration Sensor Performance on Vibration Tools by Using a Fuzzy Logic Method," SciTePress, 2020.
[11] T. H. Nasution, M. A. Muchtar, I. Siregar, and U. Andayani, "Electrical Appliances Control Prototype by Using GSM Module and Arduino," Proc. 4th Int. Conf. on Industrial Engineering and Application, 2017.
[12] [12] R. Piyare, "Internet of Things: Ubiquitous Home Control and Monitoring System Using Android-Based Smart Phone," Int. J. of Internet of Things, vol. 2, no. 1, pp. 5–11, 2013.
[13] Espressif Systems, "ESP32 Series Datasheet," 2023.
[14] Espressif Systems, "ESP32-CAM Technical Reference Manual," 2023. [Online].
[15] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Trans. on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004.
[16] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," IEEE Computer, vol. 48, no. 11, pp. 76–84, Nov. 2015.