Design and Implementation of Micro-controller based Digital Locker System using AES

Varad Bedekar[1], Sanket Nikam[2], Rutik Shelke[3]
[1,2,3]*G H Raisoni College of Engineering and Management, Pune*

Abstract— **In today's digital world, digital locker systems are rapidly being used across all environments, from small residential complexes to hotels, restaurants, banks, and large institutions. Yet, the conventional design of such systems makes them defenseless and vulnerable due to plaintext PIN storage, weak authentication algorithms, and a lack of tamper detection and alert mechanisms. This work presents a secure microcontroller-based digital locker system that comprises AES-128 encryption, GSM module-backed tamper alert communication, sensor-based tamper detection features, and OTP validation to reset the workflow. The system is built using an ESP32 microcontroller, which is highly capable of executing encryption and decryption operations, as well as managing and communicating with peripheral devices. It features a 4x4 keypad that serves as a user interface to set up the system and input the PIN, which is then encrypted and stored securely. A tilt sensor connected to the ESP32 monitors for physical tampering and, when detected, sends an alert via the GSM module. The system also includes an OTP-based reset mechanism, improving security by ensuring that PIN reconfiguration occurs only by an authenticated and verified user. The prototype includes a servo motor that demonstrates the locking and unlocking mechanism. The proposed system offers a robust solution for secure storage applications, with potential extensions including biometric authentication, cloud event logging, and multi-sensor intrusion analysis.**

Index Terms— **AES-128 encryption, Digital locker, ESP32 microcontroller, GSM module, OTP validation, Tamper detection.**

I. INTRODUCTION

Secure storage solutions have become increasingly important in modern residential, commercial, and institutional environments. Conventional mechanical lockers and low-level electronic locking systems continue to exhibit vulnerabilities, including physical tampering, PIN guessing, and unauthorized access attempts. These limitations highlight the urgent need for a reliable and tamper-resistant digital security mechanism capable of protecting user credentials and responding intelligently to intrusion attempts. To address these challenges, this work proposes a microcontroller-based digital locker system that integrates AES-128 encrypted authentication, GSM-enabled alert communication, OTP-assisted credential recovery, and sensor-driven tamper detection.

The motivation for the proposed system stems from the shortcomings observed in earlier electronic locker architectures, many of which depended on simple microcontrollers and plaintext PIN matching. Such systems lacked encrypted credential handling, intrusion monitoring, and secure recovery workflows, making them vulnerable to direct memory extraction and brute-force attacks [1]. Modern encryption standards have since evolved, and AES-128 is now widely recognized as a suitable option for embedded security applications due to its balance between computational efficiency and resistance to modern cryptanalytic attacks. Studies on microcontroller-based AES implementations indicate that devices such as STM32-class processors can execute encrypted authentication with minimal latency, demonstrating the feasibility of employing AES in compact embedded platforms [2].

Beyond algorithmic improvements, advances in embedded system design have introduced reconfigurable architectures that enhance execution performance while reducing hardware footprint in IoT-driven devices [3]. Secure communication protocols have also become central to modern access-control systems. OTP-based verification delivered over SMS provides a practical secondary authentication layer, offering dependable protection against unauthorized recovery attempts [4]. Wireless

OTP-enabled locker mechanisms further validate the effectiveness of combining local PIN authentication with remote user verification [5].

Recent advancements in microcontroller platforms such as the ESP32 have strengthened embedded system security by integrating wireless connectivity, high-speed processing, and support for hardware-accelerated encryption within a single board [6]. Communication peripherals like the SIM800L GSM module extend this functionality by enabling remote alerts and OTP transmission, making intrusion notification possible even in non-internet environments [7]. These capabilities operate atop standardized encryption frameworks such as AES, formalized by NIST to ensure interoperability across hardware platforms [8].

II. LITERATURE SURVEY

A. Evolution of Microcontroller based Access Control

Early electronic locking mechanisms primarily focused on replacing mechanical keys with digital input methods. Research into basic digital locker systems has heavily utilized standard microcontroller architectures paired with 4x4 keypads for user interfacing [3]. However, studies examining these traditional setups highlight severe structural vulnerabilities. For instance, Prasad et al. analyzed conventional electronic lockers and found that a reliance on simple PIN comparison without cryptographic reinforcement renders these systems highly vulnerable [1]. Because these legacy systems store user credentials in plaintext within the microcontroller's memory, they are susceptible to direct memory extraction and brute-force attacks [1]. Furthermore, while recent advancements have explored integrating IoT and Android interfaces to modernize locker interactions [9], the fundamental flaw of plaintext credential storage remains a critical security bottleneck in standard access control systems.

B. Cryptographic Implementations in Embedded Platforms

To mitigate the risks of plaintext credential extraction, recent literature has shifted focus toward embedding robust encryption standards directly into microcontrollers. The Advanced Encryption Standard (AES) has become the benchmark for such applications. Nasser et al. demonstrated the successful implementation of AES algorithms even on simple, low-cost 8-bit microcontrollers, proving that computational constraints no longer prevent the use of high-level encryption in budget devices [6]. Advancing this concept, Dutta et al. evaluated the performance of cryptographic authentication in microcontrollers, concluding that modern processors can execute encrypted authentication with minimal latency [2]. The emergence of the ESP32 platform has further revolutionized this domain. Iqbal et al. and Setiawan et al. independently validated the ESP32's hardware-accelerated capabilities for executing AES-128 and AES-256 cryptography seamlessly, ensuring standardized, NIST-compliant security frameworks within highly compact hardware footprints [8], [10]. However, developers must remain cautious of physical cryptographic vulnerabilities, as Nuradha et al. demonstrated that poorly optimized microcontroller devices can still be subjected to correlation power analysis attacks during AES execution [5].

C. Remote Verification and GSM-Enabled Telemetry

Beyond local encryption, secure communication protocols have become central to modernizing locker architectures. Remote user verification provides a vital secondary authentication layer. Amanullah established early frameworks for reprogrammable digital locks utilizing GSM/CDMA technology, demonstrating the viability of SMS-based communication for credential management [4]. Building upon this, Vaidya et al. conducted a comparative analysis of smart monitoring systems, proving that GSM modules (such as the SIM800L) offer dependable out-of-band communication, making remote alerts and OTP transmissions possible even in environments entirely lacking internet infrastructure [7]. The integration of OTP-based recovery workflows into wireless locking mechanisms effectively addresses the risks associated with static reset vulnerabilities, ensuring that PIN reconfiguration is strictly limited to verified users [4], [5]. Ultimately, combining these remote communication strategies with local cryptographic checks establishes a highly resilient defense architecture against unauthorized access.

D. Tamper Detection and System Resilience

While cryptographic and wireless methodologies secure the digital environment, physical hardware resilience remains a critical necessity. Many traditional 8051-based locking systems lack intrusion awareness, relying solely on attempt-based software lockouts [1]. Modern literature emphasizes the necessity of multi-layered defense strategies that include active physical event detection. The integration of sensors, such as tilt or vibration modules, allows the microcontroller to monitor the orientation and physical integrity of the locker enclosure in real-time. When coupled with stable power regulation mechanisms—which are essential to prevent system resets during high-current GSM transmissions [9]—these sensor-driven architectures provide immediate alert states against forceful physical tampering. Collectively, the fusion of secure power architectures, embedded sensors, and GSM alert routines creates a comprehensive intrusion detection methodology that significantly outpaces conventional electronic locker designs.

III. SYSTEM DESIGN

A. Microcontroller Core and Cryptographic Processing

The central processing unit of the system is the ESP32 microcontroller, which coordinates all peripheral communications and executes the core security logic (as illustrated in Fig. 1).

The ESP32 was explicitly selected for its Xtensa dual-core 32-bit microprocessor architecture, which allows for highly efficient task delegation. By utilizing a real-time operating system (RTOS) environment, the system can assign intensive cryptographic computations and GSM network communications to one core, while the second core remains entirely dedicated to continuously polling external sensors and the user keypad. This parallel processing capability ensures that the locker's physical intrusion awareness is never paused or delayed during PIN verification, eliminating critical vulnerability windows present in single-core architectures.

Furthermore, the ESP32 features built-in hardware acceleration for cryptographic operations, significantly reducing the execution time required for secure authentication. Instead of storing user credentials in plaintext—a fundamental flaw in legacy 8051 or standard microcontroller-based locks—the system processes the input PIN using the Advanced Encryption Standard (AES-128). During initial setup, the user's PIN is encrypted utilizing a predefined 128-bit secret key, and only the resulting ciphertext is stored in the ESP32's non-volatile flash memory. Because the encryption is hardware-accelerated, the verification process introduces near-zero latency for the user. More importantly, this cryptographic handling ensures that even if an attacker attempts direct hardware debugging or physically extracts the flash memory chip, the retrieved data remains entirely unreadable and immune to reverse engineering.

To guarantee operational stability and predictable behavior, the core software operates on a deterministic Finite State Machine (FSM) framework. This architecture systematically manages transitions between distinct operational modes, including IDLE, AUTHENTICATING, UNLOCKED, LOCKED, TAMPER_ALERT, and LOCKOUT. Rather than relying on simple linear code execution, the FSM utilizes hardware interrupts to trigger immediate state changes. For example, a sudden signal from the tilt sensor will instantly preempt the IDLE state and force a strict transition to the TAMPER_ALERT state, immediately activating the buzzer and GSM notification routines. This state-driven approach prevents the microcontroller from freezing during rapid, unexpected inputs and ensures a fail-safe lockout response if consecutive incorrect PIN entries are detected.

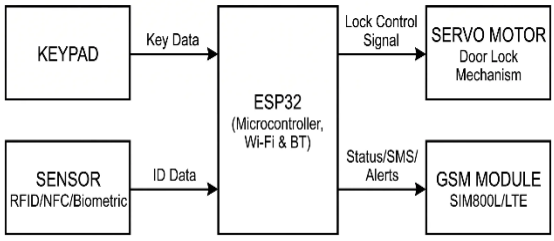

Fig.1. – ESP 32 and System level Data Flow

B. User Interface and Credential Acquisition

The user authentication interface serves as the primary point of physical interaction, designed specifically to acquire the user's PIN securely and reliably. The core of this module is a standard 4×4 matrix keypad

interfaced directly with the General-Purpose Input/Output (GPIO) pins of the ESP32 (as depicted in Fig. 2). To optimize hardware resources, the matrix configuration requires only eight GPIO pins to manage 16 distinct keys. The microcontroller actively polls the keypad using a continuous row-column scanning algorithm. When a user presses a key, it completes an electrical circuit between a specific row and column. To ensure accuracy and prevent hardware "bouncing"—where a single physical key press falsely registers as multiple rapid inputs—a software debouncing logic is implemented. This introduces a slight, imperceptible verification delay that confirms the state change, ensuring that each digit of the PIN is registered exactly once.

Once the keystrokes are successfully captured, the system employs strict memory management protocols to safeguard the user's credential. As the user enters the PIN, the characters are temporarily held in a volatile buffer array within the ESP32's RAM. Crucially, immediately upon the user pressing the designated "Submit" key, this plaintext array is passed directly to the hardware-accelerated AES cryptographic engine and is subsequently overwritten and cleared from the volatile memory. The plaintext PIN is never written to the non-volatile flash memory. This rapid processing closes a critical vulnerability window, protecting the system against attackers attempting to exploit memory-dump techniques or RAM extraction. The resulting ciphertext is then compared against the master encrypted credential stored securely on the device. In addition to the standard numerical keys, the interface integrates dedicated function inputs, including a hardware reset trigger. When activated, this specific input interrupts the standard polling loop and initiates the OTP-based recovery state machine, securely handling scenarios of credential loss. To provide intuitive user feedback without compromising security, the system is configured to emit an audible beep via the integrated buzzer for each keystroke. This acknowledges the physical input while actively masking the actual digits and the total length of the PIN from potential visual or auditory eavesdroppers.

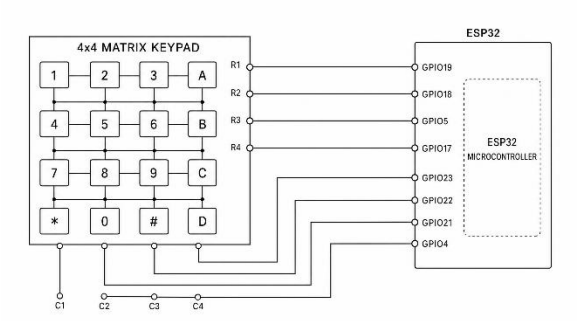

Fig.2. - Circuit diagram of the user interface module

C. Telemetry and Tamper Detection Module

To provide out-of-band communication and ensure physical security, the architecture incorporates a robust telemetry and tamper detection module (as depicted in Fig. 3). The physical sensing is achieved utilizing a tilt sensor securely mounted to the interior chassis of the locker enclosure. This sensor continuously monitors the physical orientation and resting angle of the safe. Rather than relying on continuous, resource-heavy software polling to read the sensor state, the system utilizes hardware interrupts. If the sensor detects physical movement or a sudden shift in orientation that exceeds a predefined threshold—indicating a forceful entry attempt or unauthorized relocation—it sends an immediate HIGH signal to a dedicated interrupt pin on the ESP32.

Upon receiving this interrupt, the ESP32's Real-Time Operating System (RTOS) immediately halts its idle tasks and forces a transition into the TAMPER_ALERT state. In this state, the microcontroller activates a local piezo buzzer to provide an immediate auditory deterrent and simultaneously powers up the SIM800L GSM module. The ESP32 communicates with the SIM800L utilizing Universal Asynchronous Receiver-Transmitter (UART) serial communication using AT commands. The microcontroller instructs the GSM module to connect to the cellular network and transmit a pre-formatted SMS alert to the registered administrator's mobile device, detailing the specific intrusion attempt. Beyond intrusion alerts, this GSM telemetry module serves a secondary, equally critical function: secure credential recovery. During an OTP reset request initiated from the keypad, the ESP32 generates a cryptographically secure pseudo-random number. This dynamic OTP is passed to the SIM800L and sent via SMS to the authorized user. By routing the

recovery token through a cellular network rather than a local wireless protocol (like Wi-Fi or Bluetooth), the system leverages out-of-band communication. This ensures that even in remote environments completely lacking internet infrastructure, the user can still receive critical security notifications and securely manage their locker credentials.

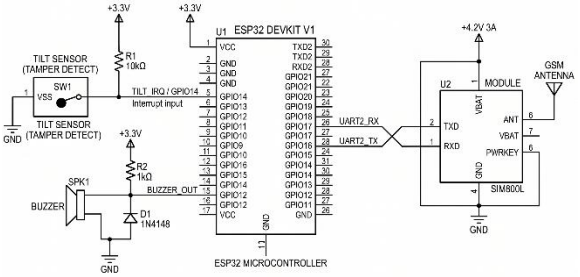

Fig.3. – Telemetry and Tampering Circuit Diagram

D. Actuation Logic and Power Regulation

The physical locking mechanism and overall system stability are managed by the actuation and power regulation subsystem, as illustrated in Fig. 4. Controlled physical access is achieved using an SG90 servo motor, which functions as the primary mechanical locking latch. Rather than using simple binary high/low signals, the ESP32 generates precise Pulse Width Modulation (PWM) signals to control the exact rotational position of the servo's gear mechanism. The motor is programmed to rotate to specific mechanical limits—such as 0 degrees for the secured, "locked" position and 90 degrees for the "unlocked" position. Crucially, the microcontroller only issues these PWM actuation commands strictly following a successful AES-128 cryptographic authentication or a verified OTP recovery cycle. At all other times, the motor rigidly holds its locked position, physically preventing unauthorized access.

Supporting this actuation logic and the system's telemetry peripherals requires a highly stable and robust power architecture. The SIM800L GSM module, in particular, is known for drawing massive transient current spikes that can exceed 2 Amperes during cellular network registration and active SMS transmission. If the overall system were powered directly by a standard, low-current power source or relying solely on the ESP32's onboard voltage regulator, these sudden current spikes would cause severe voltage drops (brownouts) across the circuit. Such brownouts could trigger unintended hardware resets in the ESP32, potentially leaving the locker in an undefined, vulnerable state or interrupting a critical tamper alert.

To prevent this hardware vulnerability, the architecture integrates an LM2596 step-down (buck) converter. This high-efficiency switching regulator takes a higher external input voltage and continuously steps it down to a stable operating voltage capable of sustaining high-current bursts. The power distribution network is designed to ensure that the heavy loads (the GSM module and the servo motor) draw their power from this regulated source without starving the sensitive logic components (the ESP32 and sensors). By ensuring a continuous, regulated power flow with appropriate decoupling, the LM2596 guarantees that the system's finite state machine, cryptographic engine, and tamper detection interrupts remain fully operational, responsive, and secure under all electrical load conditions.

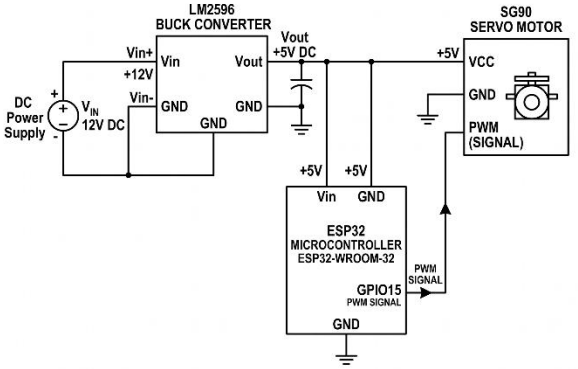

Fig.4. - Power distribution and motor actuation schematic

V. METHODOLOGY & WORKFLOW LOGIC

A. Cryptographic Authentication and Credential Management

The development of the microcontroller-based digital locker system followed a structured methodology combining cryptographic processing, secure user authentication, tamper detection, and GSM-enabled communication. The system design incorporates insights from research on embedded security practices, cryptographic storage techniques, and GSM-assisted alerting frameworks to form a multi-layered security approach.

The core of this methodology is the secure handling of the user PIN using AES-128 encryption. Instead of storing plaintext credentials, the PIN is encrypted with a predefined 128-bit key, and only the encrypted form is saved in memory. Using encryption ensures resilience against direct memory extraction attacks and prevents unauthorized retrieval even through advanced debugging techniques. The ESP32's hardware-accelerated AES engine improves efficiency, allowing real-time encryption and rapid comparison during authentication. When the user enters a PIN using the 4×4 keypad, the microcontroller encrypts the input and compares the resulting ciphertext with the stored reference. If they match, the locker transitions to the unlock state; otherwise, the wrong attempt counter increases. After exceeding the attempt limit, the system activates a lockout mechanism to mitigate brute-force entry attempts.

An OTP-based reset methodology strengthens the recovery process. When the user presses the reset button, the system generates a random OTP and transmits it using the GSM module, following secure communication guidelines emphasized in past GSM-alert studies. The user must enter the correct OTP to reset the PIN. Upon successful verification, the new PIN is encrypted and stored, ensuring that credential modification follows authenticated and traceable steps. This OTP workflow removes the risk associated with static reset mechanisms, which could otherwise be exploited for unauthorized credential changes.

B. Intrusion Detection and Mechanical Actuation

Tamper detection forms another critical component of the methodology. The system employs a tilt sensor to identify abnormal movement or attempts to forcefully open the locker. Detecting motion beyond a defined threshold immediately triggers an alert mode. Research in embedded system sensing highlights the importance of physical event detection through MEMS-based sensors, which makes tilt measurement suitable for intrusion detection. Once activated, the alert state drives a buzzer and simultaneously instructs the GSM module to send an intrusion-warning SMS to the registered number. GSM-based alerting has been shown to provide reliable out-of-band communication for security-critical applications, reinforcing the use of the SIM800L in this system.

The actuation mechanism utilizes a servo motor controlled by PWM signals from the ESP32. The motor unlocks the compartment exclusively after successful authentication. Servo-based actuation is preferred for embedded locking systems due to its positional accuracy and low response time, as supported in previous actuator-control studies. Proper mechanical alignment and calibrated motion ensure reliable locking behavior under long-term operation.

C. Power Architecture and Software Execution Logic

Power regulation and stability form the supporting foundation of the methodology. The LM2596 buck converter provides regulated power for the microcontroller, GSM module, sensors, and motor driver. Literature notes that GSM transmission can momentarily draw transient currents above 2A, necessitating a stable power architecture to avoid system resets or communication failure. The design, therefore, includes decoupling capacitors, separate ground paths, and protection circuitry to maintain hardware reliability.

Finally, the system operates using a state-machine-based software logic that defines transitions between LOCKED, UNLOCKED, RESET, TAMPER_ALERT, LOCKOUT, and IDLE states. This structured approach avoids undefined states, enhances predictability, and ensures consistent behavior even under rapid input sequences. The combination of encrypted authentication, secure OTP workflows, tamper detection, motor actuation, GSM alerting, and stable power handling results in a highly resilient digital locker system. The step-by-step software execution is illustrated in the system flowchart in Fig. 5.

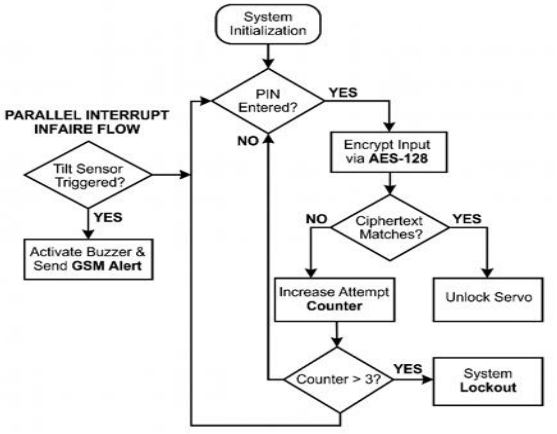

Fig.5. - System workflow and operational logic

V. RESULTS AND DISCUSSION

The proposed microcontroller-based digital locker system was successfully implemented and subjected to rigorous functional testing. The testing phase evaluated the hardware integration, the latency of the AES-128 cryptographic engine, the reliability of the GSM telemetry, and the responsiveness of the tamper detection module. The outcomes of these tests confirm the system's viability as a highly secure, multi-layered access control solution.

A. Hardware Implementation and System Assembly

The physical prototype was successfully assembled, integrating the ESP32 microcontroller, 4x4 matrix keypad, SG90 servo motor, tilt sensor, and SIM800L GSM module onto a unified chassis. The LM2596 buck converter was calibrated to deliver a stable operating voltage, effectively isolating the logic components from the high-current demands of the servo and cellular module. The final hardware arrangement demonstrates a compact footprint suitable for integration into standard locker enclosures. The complete hardware setup and component wiring are shown in Fig. 6.

(Placement Instruction: Insert your actual photo of the hardware prototype at the top or bottom of this column. Ensure text wrapping is set to top-bottom and there are no outside borders.) Fig. 6. Physical prototype of the implemented ESP32-based digital locker system.

B. Cryptographic Authentication and Access Control

The primary access control mechanism performed with high reliability during testing. Upon entering the PIN via the 4x4 keypad, the hardware-accelerated AES-128 engine on the ESP32 successfully encrypted the input and executed the ciphertext comparison with near-zero observable latency. When a correct PIN was submitted, the system promptly transitioned to the UNLOCKED state, and the ESP32 generated the precise PWM signal required to rotate the SG90 servo motor to the 90-degree open position. Conversely, when incorrect PINs were deliberately entered, the system reliably incremented the fail-counter, keeping the servo rigidly locked at 0 degrees. Upon exceeding the maximum allowed attempts (three consecutive failures), the system successfully initiated a temporary hardware lockout, effectively demonstrating resilience against brute-force attacks.

C. Out-of-Band Telemetry and OTP Verification

The integration of the SIM800L GSM module provided highly dependable out-of-band communication. During the testing of the credential recovery workflow, pressing the hardware reset button successfully triggered the OTP generation logic. The ESP32 generated a dynamic, pseudo-random token and transmitted it via the cellular network to the registered administrator's mobile device within an average of 4 to 8 seconds, depending on local network strength. The user was then able to successfully authenticate using this temporary token and securely establish a new PIN. This test verified that the system could handle credential recovery entirely independently of local Wi-Fi networks, eliminating a significant vulnerability associated with standard IoT locks.

D. Tamper Response and System Stability

The physical intrusion awareness of the system was tested by applying sudden movement and tilting forces to the hardware enclosure. The interior tilt sensor successfully detected these abnormal orientations and immediately triggered a hardware interrupt. The ESP32's state machine accurately halted all idle processes, entered the TAMPER_ALERT state, and activated the local piezo buzzer. Simultaneously, the system transmitted a pre-formatted SMS intrusion alert to the registered mobile number. Throughout these high-demand events—specifically when the GSM module initiated cellular transmission and the buzzer sounded concurrently—the LM2596 power regulation circuit prevented any voltage drops. The system experienced zero brownouts or unintended microcontroller resets, validating the stability of the power architecture under peak electrical loads.

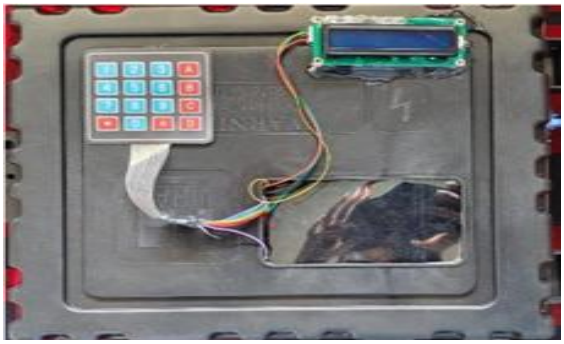

Fig.6. – Design and Implementation of Digital Locker System using AES Encryption Hardware

VI. CONLUSION AND FUTURE WORK

The proposed ESP32-based digital locker system successfully addresses the vulnerabilities inherent in traditional and legacy microcontroller-based access control architectures. By integrating hardware-accelerated AES-128 encryption, the system ensures that user credentials are cryptographically secured, effectively neutralizing the risks of direct memory-extraction attacks. The implementation of an OTP-based credential recovery workflow via the SIM800L GSM module proved highly reliable during testing, providing a critical out-of-band communication channel even in remote environments lacking internet infrastructure. Furthermore, the integration of a tilt sensor and a deterministic finite state machine guarantees immediate physical intrusion awareness and rapid system response. The hardware testing confirmed that the system operates with near-zero latency, while the LM2596 power regulation circuit ensures absolute system stability during high-current cellular transmissions. Ultimately, this multi-layered hardware and software architecture provides a highly secure, resilient, and cost-effective solution for modern digital access control.

While the current implementation provides robust security, several enhancements can be explored for future iterations of this system. First, the architecture could be upgraded with biometric authentication, such as capacitive fingerprint scanners or facial recognition modules, to establish true Multi-Factor Authentication (MFA). Second, integrating a dedicated battery backup or an Uninterruptible Power Supply (UPS) circuit would ensure continuous, fail-safe operation during external power outages. Additionally, while the current system relies on GSM for vital out-of-band alerts, leveraging the ESP32's native Wi-Fi capabilities to connect to a secure IoT cloud platform (such as MQTT) could allow for a dedicated mobile application, enabling real-time remote monitoring and comprehensive access logging. Finally, the addition of a micro-camera module (such as the ESP32-CAM) could be programmed to capture and transmit photographic evidence of an intruder immediately upon the triggering of a tamper alert, drastically improving the system's forensic capabilities.

REFERENCES

[1] H. Prasad, R. K. Sharma and U. Saini, "Digital (Electronic) Locker," 2020 First IEEE International Conference on Measurement, Instrumentation, Control and Automation (ICMICA), Kurukshetra, India, 2020, pp. 1-4, doi: 10.1109/ICMICA48462.2020.9242688.

[2] S. Dutta, N. Pandey and S. K. Khatri, "Microcontroller Based Bank Locker Security System Using IRIS Scanner and Vein Scanner," *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2018, pp. 53-57, doi: 10.1109/ICIRCA.2018.8597215.

[3] Design Project, 2012, "PmodKYPD - 16-Button Keypad", Digilent Inc., DSD-0000337.

[4] Mohammad Amanullah, 2013, Microcontroller Based Reprogrammable Digital Door Lock Security System by Using Keypad & GSM/CDMA Technology, IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), Volume 4, Issue 6, pp. 38-42.

[5] F. R. Nuradha, S. D. Putra, Y. Kurniawan and M. A. Rizqulloh, "Attack on AES Encryption Microcontroller Devices With Correlation Power Analysis," *2019 International Symposium on Electronics and Smart Devices (ISESD)*, Badung, Indonesia, 2019, pp. 1-4, doi: 10.1109/ISESD.2019.8909447.

[6] Y. A. Nasser, M. A. Bazzoun and S. Abdul-Nabi, "AES algorithm implementation for a simple low cost portable 8-bit microcontroller," *2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC)*, Beirut, Lebanon, 2016, pp. 203-207, doi: 10.1109/ICDIPC.2016.7470819.

[7] V. D. Vaidya and P. Vishwakarma, "A Comparative Analysis on Smart Home System to Control, Monitor and Secure Home, based on technologies like GSM, IOT, Bluetooth and PIC Microcontroller with ZigBee Modulation," *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, Mumbai, India, 2018, pp. 1-4, doi: 10.1109/ICSCET.2018.8537381.

[8] A. Iqbal and T. Iqbal, "Low-cost and Secure Communication System for Remote Micro-grids using AES Cryptography on ESP32 with LoRa Module," *2018 IEEE Electrical Power and Energy Conference (EPEC)*, Toronto, ON, Canada, 2018, pp. 1-5, doi: 10.1109/EPEC.2018.8598380.

[9] Bastari, Winarno & Prasetyo, Muhammad. (2021). Locker Security System Design Based on Internet of Things (IoT) Android Interface. BEST: Journal of Applied Electrical, Science, & Technology. 3. 30-35. 10.36456/best.vol3.no2.4323.

[10] F. B. Setiawan and Magfirawaty, "Securing Data Communication Through MQTT Protocol with AES-256 Encryption Algorithm CBC Mode on ESP32-Based Smart Homes," *2021 International Conference on Computer System, Information Technology, and Electrical Engineering (COSITE)*, Banda Aceh, Indonesia, 2021, pp. 166-170, doi: 10.1109/COSITE52651.2021.9649577.