JOURNAL OF INFORMATION TECHNOLOGY AND COMPUTER ENGINEERING
https://jitce.fti.unand.ac.id | e-ISSN: 2599-1663

Prototyping of a Smart, Secure and Multipurpose Flash Pen Drive

Benjamin Kommey [1], Prosper Ocloo Nulako Kwaku[1], Gabriel Ib-Nemwin Peguu [1], Daniel Opoku [1], Kwame Agyeman Prempeh Agyekum [1*]

[1]*Faculty of Electrical and Computer Engineering, Kwame Nkrumah University of Science and Technology Kumasi, Ghana*
Corresponding author: bkommey.coe@knust.edu.gh

***Abstract*—This paper proposed a non-traditional pen-drive that incorporates biometric authentication, wireless file access, encryption, and the display of feedback within a compact embedded device. The designed prototype is based on a dual microcontroller architecture, using the STM32 as the master controller for system logic and security, and the ESP32-WROOM for wireless connectivity and mobile interaction. The system includes a custom communication protocol between the two microcontrollers to ensure synchronized behavior between authentication and Wi-Fi access. Two physical models were envisioned and prototyped: one using buttons and a compact OLED display, and another with a touchscreen interface for advanced control. This report outlines the methods, system architecture, PCB design, firmware logic, and testing strategies. While the prototype is still under development, the design has been validated via simulation, testing, and real-world power and thermal calculations. This work demonstrates the feasibility of building a modern, user-friendly USB drive that merges data security, IoT accessibility, and mobile independence**

***Keywords*— Flash drive; USB; Secure; Multipurpose; Portable**

Manuscript received 13 Feb 2026; revised 21 May 2026. Date of publication 8 Jun 2026.

I. INTRODUCTION

Flash drives, popularly called pen-drives, are one of the everyday tools for carrying and transferring user data. They are affordable, easy to use, and capable of storing large amounts of information. However, despite how far technology has advanced, most flash drives still work the same way they always have. They have not evolved to meet modern expectations for smart functionality, mobility, or security. In today's world, data privacy and convenient access are more important than ever. Many people now use flash drives to store sensitive documents such as school work, personal photos, health records, legal files, or business materials. Unfortunately, traditional flash drives offer very little protection. If one is lost or stolen, the data it holds can be easily accessed by anyone.

As smartphones, wireless technology, and smart devices become more common in everyday life, people now expect better features even from simple tools like flash drives. One of the main inspirations for this project was the idea of giving the flas drive its own screen. While most flash drives are silent and inactive until plugged into a computer, a built-in display would allow the device to communicate with the user. It could show how much storage space is used or available, the current battery level, Wi-Fi status, charging state, or even progress during file transfers. This makes the device more interactive and informative, giving the user better control and awareness, all without needing to plug it into anything.

This work builds on the core idea and adds extra modern features to create a smart and secure flash drive. These features include wireless access through a mobile app, so users can connect and manage their files without needing a laptop or desktop. Fingerprint authentication is included to prevent unauthorized access, and encryption ensures that stored data stays private and secure. The device is powered by a rechargeable battery, making it completely portable and functional on its own.

Additionally, traditional flash drives give the user no way of knowing what's happening inside the device unless it is connected to a host computer. You can't check how much space is left, whether it's charging, or if a file transfer is still in progress. This makes the device feel outdated in a world where even basic gadgets like smart watches and earbuds provide real-time feedback. In many situations when a pc is unavailable, or when working from a mobile device, this creates unnecessary limitations. People now expect wireless access, remote control, and compatibility with mobile apps, yet this level of convenience is absent in most storage device and there is no standard solution that brings all of these features together into one device. Users often have to rely on multiple tools or devices to meet these needs, which can be inconvenient and less secure. This project addresses these

issues by aiming to build a smart, secure, and portable flash drive.

Many literatures were reviewed and related works carefully studied and presented in this section. In [1], a secure encryption-based hardware device designed to protect sensitive data was presented and serves as a critical reference for understanding secure key management, encryption workflows, and embedded system-level authentication. The patented device introduces a method for reconstructing encryption keys without storing them directly in memory. It achieves this through Shamir's Secret Sharing scheme, which divides a secret into multiple smaller parts that are distributed across the device and/or external systems. A certain number of these shares are required to reconstruct the original key. This means that even if an attacker gains access to some parts of the system, the full key remains unrecoverable unless the threshold number of shares is met. [2] presents a project aimed at improving file sharing between USB drives by introducing wireless capabilities and a built-in user interface. The device is a portable peripheral unit designed to act as a wireless transfer hub between external USB flash drives and SD cards. It includes a microcontroller-based control unit, basic UI navigation through a touchscreen, and embedded software to detect connected drives and manage file transfers. In [3], a comprehensive evaluation of several commercial "secure" USB flash drives from manufacturers including Samsung, LG, SanDisk, and Imation were studied. The purpose of the study was to test how effective these devices were at protecting sensitive user data from unauthorized access, especially in scenarios involving device loss or physical tampering. The inclusion of biometric authentication, on-device encryption, and tamper detection directly addresses the vulnerabilities documented in the paper.

Paper [4], is a highly integrated wireless microcontroller designed specifically for low-power, high-performance embedded applications. The ESP16 features a dual-core Tensilica LX6 processor, allowing it to handle multiple operations simultaneously. This structure reduces latency and increases responsiveness during file browsing or wireless transfers. The ESP16 supports a full TCP/IP network stack, including HTTP, HTTPS, FTP, and mDNS protocols and enables the device to act as a mini web server, allowing file access and management through a smartphone or browser interface. These features ensure that all communication between the flash drive and the user's mobile device is secure, even during wireless file transfers or over-the-air (OTA) firmware updates. In [5], the STM32 microcontroller, a 16-bit ARM Cortex-M3 MCU designed for performance, low power consumption, and robust control in embedded applications was used. The STM32 functions as the main controller of the smart pen drive system, taking responsibility for security, USB communication, display handling, and user authentication. In device mode, the STM32 can emulate a Mass Storage Class (MSC) device, allowing standard file read/write operations. With its low cost, broad support, and proven reliability, the STM32 enables this project to integrate strong local security, interactive feedback, and efficient system control and all within the size and power limitations of a portable USB flash drive. In [6] explores in depth how embedded devices generate heat and how it can be effectively managed without using fans or large heatsinks thus making it highly relevant to compact, battery-powered projects like this smart pen-drive. The work focuses on dynamic thermal management (DTM), a method of predicting and controlling heat generation by adjusting how the system operates in real time. This is especially important in small embedded systems that need to stay cool while still delivering performance and protecting internal components.

II. METHOD

A structured engineering approach was used as the methodology for this work. It begins with extensive research which informed the planning, design choice, implementation strategies, testing and evaluation. Initially, a search and selection of suitable hardware components was undertaken. This involves the choice of microcontrollers, memory chips, wireless modules, biometric sensors, display, and power management circuits. Each selected component is evaluated based on compatibility, power efficiency, size, cost, and ability to meet the functional requirements of the desired system. Later, the system prototype architecture was designed and developed. Detail description of the designed system architecture is presented before.

A. The System Design Architecture

The system design architecture as shown in Figure 1, uses an STM32 [5],[9] to serve as the main controller responsible for data storage, encryption, and interfacing with the user. An ESP32 [4],[7],[8] is used to handle wireless communication and interaction with a companion mobile software application. A master–slave model is considered, where the STM32 issue commands and manage security, while the ESP32 handles file serving and device discovery over Wi-Fi. The design system includes a fingerprint sensor for user authentication, and a real-time clock and flash memory for secure data storage. Data was protected using AES encryption and managed at the firmware level. A display was integrated to provide visual feedback, showing important status updates such as storage usage, battery life, transfer progress, and connection status. A rechargeable battery was used to power the entire system, with a power management circuit, including a charging module and voltage regulator to ensure safe and efficient operation [13], [18]. The use of the battery allows the device to work independently without needing to be plugged into a computer.

Two different physical prototypes were developed and compared: one with a compact OLED display and physical navigation buttons, and another using a touchscreen TFT for a more interactive experience. Custom PCBs were designed using Eagle, and conceptual 3D models of the enclosure were created to support the intended use and internal layout. Finally, the designed system was tested for functionality, user experience, power consumption, and thermal stability. Heat and battery performance were monitored, and optimization techniques like dynamic sleep modes and thermal triggers were considered [18], [19].

One of the main goals of this project is to make the pen drive work without needing to plug it into a computer. To do that, it needs a way to connect wirelessly to other devices like smartphones or tablets. This is made possible using two

popular wireless technologies: Wi-Fi and Bluetooth, both of which are built into the ESP32 microcontroller used. A user can connect to this network using the smartphone, open an application, and access the files stored on the device. This is very useful because it removes the need for a computer and gives users more flexibility. The Bluetooth option is good for sending small messages or setting up a connection quickly. These wireless methods are important because they make the flash drive smarter and more flexible. Instead of only working when it's plugged into a USB port, it can now work like a smart device that users can connect to and control from a distance. Using Wi-Fi and Bluetooth together makes the device feel more modern and easier to use in everyday situations.

As people carry more private and sensitive information on their flash drives, security becomes a major concern [3], [16], [20]. If one loses a drive or it gets stolen, anyone could plug it into a computer and see all the files in it, unless there is some way to lock and protect the data. To solve this problem, this project uses encryption and biometric authentication for data safety. The developed flash drive uses AES, a strong and trusted encryption method that is widely applied in the technology industry, including in banking and military systems [10]. AES runs directly on the device using the STM32 microcontroller, and for that matter, data is protected even before storage. Biometric authentication adds another layer of protection. Instead of using a password, the flash drive uses a fingerprint sensor to check if the person trying to access the data has ownership [15]. Fingerprints are unique, so this method is much harder to fake or guess. The STM32 was programmed to scan and match biometric and only allow access after successful user verification. By combining encryption and fingerprint scanning, the flash drive becomes more secure [20], [21]. Even if the device is stolen, the data files can not be access without verification. This protection is especially useful for groups such as students, professionals, or whoever keeps important information on the storage device. The combination of encryption and biometric authentication makes the pen drive smart and safe.

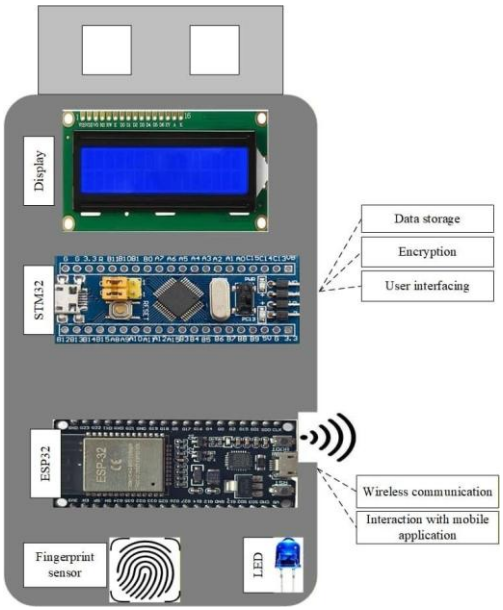


Figure 1. The designed system architecture

The project is a hybrid embedded system device combining an ESP32 module for user interaction, networking, and storage management and a STM32 microcontroller responsible for low-level control and peripheral coordination. The system integrates a TFT touch display, removable SD card storage. A serial interface is provided for communication between the two microcontrollers via a dynamic master-slave model, where control authority shifts between the ESP32 and STM32 based on operational mode, rather than maintaining a fixed master-slave relationship. The storage architecture was designed to use SD card as the primary storage medium, ESP32 SD library for file operations, and STM32 acting as a logical peer via serial synchronization rather than direct storage ownership. Unlike conventional fixed master-slave systems, control authority in this design changes at runtime depending on the active operational mode. This architecture allows both microcontrollers to independently initiate actions while maintaining orderly communication and avoiding bus contention.

B. System Block Diagram

The design system revolves around ensuring a seamless integration of all the components while maintaining a compact form factor. As shown in Figure 2, the system block diagram outlines the interconnections between each component, showcasing the whole architecture of the device. The microcontroller unit (MCU) connects and manages the power supply, memory, user interface, connectivity, and security modules, enabling efficient and secure data operations. At the core of the system is a dual microcontroller setup involving STM32, acting as the master controller for system logic, fingerprint authentication, encryption, USB handling, and user interface and the ESP32 which serves as the slave controller responsible for Wi-Fi communication, mobile software application or web interface hosting, and remote file access. The master–slave configuration isolates critical security and storage functions from external network exposure, thus minimizing risk and thereby improving performance via parallel task distribution.

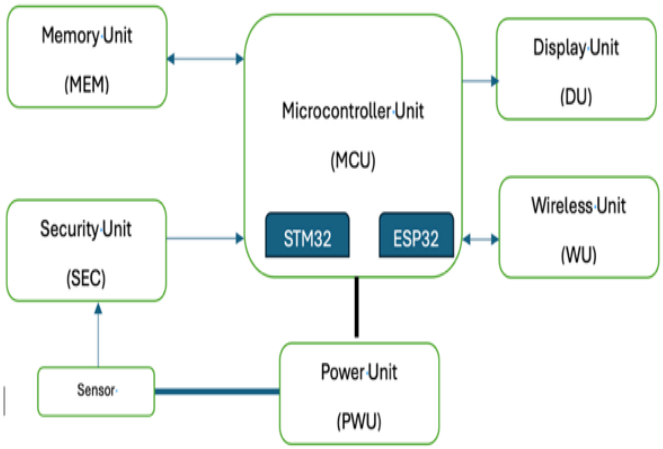


Figure 2. The designed system block diagram

The system prototype integrates the following functional modules in a cohesive structure: as contain in Table I.

TABLE I
SYSTEM MODULES AND FUNCTIONS

Module	Purpose
STM32	Handles USB, AES encryption, biometric logic, LCD display control, and overall coordination.
ESP32	Handles Wi-Fi connectivity, SoftAP creation, web server, and mobile software application data access.
Sensor (e.g. R147)	Captures and verifies user identity. Interfaces via UART with the STM32.
MicroSD	Encrypted storage directly accessed and controlled by STM32.
OLED or TFT Display	Displays device status, file transfer information, and navigation interface.
Buttons or Touch Interface	Used to navigate menus, enable/disable Wi-Fi, confirm access, or initiate transfers.
Battery + Charging Module	Ensures independent power and recharging capability via USB or DC input.
USB Interface	Enables data transfer in traditional pen or flash drive mode and recharging of internal battery.

TABLE II
SUMMARY OF OTHER FEATURES AND FUNCTIONS

Module	Type	Function
Storage	MicroSD	Primary data storage medium. Stores encrypted user files. Enables STM32-controlled read/ write operations.
Fingerprint Sensor	R145 /FPM10A	UART - User authentication. Captures and stores fingerprint templates. Verifies fingerprint before allowing access to encrypted storage or wireless sharing.
Display	OLED TFT	0.96–I2C/SPI– Model A Provides real-time user feedback. Shows storage usage, battery level, Wi-Fi state, file transfer progress, and system messages. 2.4/2.8” SPI – for Model B Interactive user interface for navigation and status. Replaces physical buttons, enabling richer UI with icons, progress bars, and file menus.
Input & Navi	Push Buttons Touch Panel	Model A. Tactile momentary switches (Up, Down, Select, Power) Navigate menus, toggle Wi-Fi, confirm file actions, power device on/off. Model B Detects taps and swipes to navigate touchscreen UI.

The display system, fingerprint authentication, and wireless modules interact indirectly through STM32's central control logic. Communication between the STM32 (master) and ESP32 (slave) is via UART, chosen for simplicity and sufficient speed for control signals. The STM32 sends structured commands to the ESP32 to perform following tasks:

- Enable or disable Wi-Fi based on user input or fingerprint or biometric verification.
- Notify successful or failed authentication.
- Authorize or reject file-sharing sessions.
- Activate low-power or emergency modes.

The ESP32 only allows access to storage after receiving explicit authorization from STM32, ensuring tight security control over wireless data access. The system designed is powered by a rechargeable lithium-ion battery. To ensure thermal stability, the STM32 and ESP32 are both configured to enter low-power/sleep modes when idle. Other features and functions are as summarized in Table II

C. System Engineering and Prototyping

Each component for the prototype design was selected for its ease of integration, support for low-power operation, small footprint, and compatibility with the STM32 and ESP32 platforms. This deliberate hardware selection ensures the device can meet its goals of security, wireless access, real-time interaction, and portability, while maintaining safety and thermal efficiency. The electronic hardware of the design was physically realized through PCB layout and mechanical housing. The dual-model nature of the project (Model A and Model B) required separate planning and layout strategies tailored to each use case, based on form factor, interaction mode (buttons vs. touch), and component space requirements. The PCB was designed using Autodesk Eagle, and enclosure designs were prototyped using Fusion 200 for CAD modeling. Key design goals included compactness, thermal efficiency, mechanical durability, and user accessibility. In developing the physical hardware for this work, the following were identified as top-level design priorities:

- Compact form factor suitable for keychain or pocket carry.
- Physical access to the biometric scanner, buttons, and display.
- Component heat isolation to prevent hotspots during wireless operation.
- Display visibility for both OLED and TFT screen variants.
- Modular layout to enable debugging, testing, and replacement of parts.
- Battery safety and accessibility for charging and maintenance.

The Eagle-designed PCB was organized using modular zones, with component separation based on signal class and power demands. The layout was implemented on a 2-layer PCB to simplify routing and reduce board cost. Figure 3 and 4 contain screen shots of the schematics and PCB designs of the prototypes.

1) Model A: Oled + Buttons Layout: Model A emphasized simplicity, minimal size, and tactile controls as images in Table III.

2) Model B: Touchscreen TFTLayout: Model B introduced a graphical touchscreen interface via a 2.4” or 2.8” TFT module, as images in Table III. It allowed for richer interaction and more dynamic control screens.

TABLE III
THE DESIGNED SYSTEM SCHEMATIC I

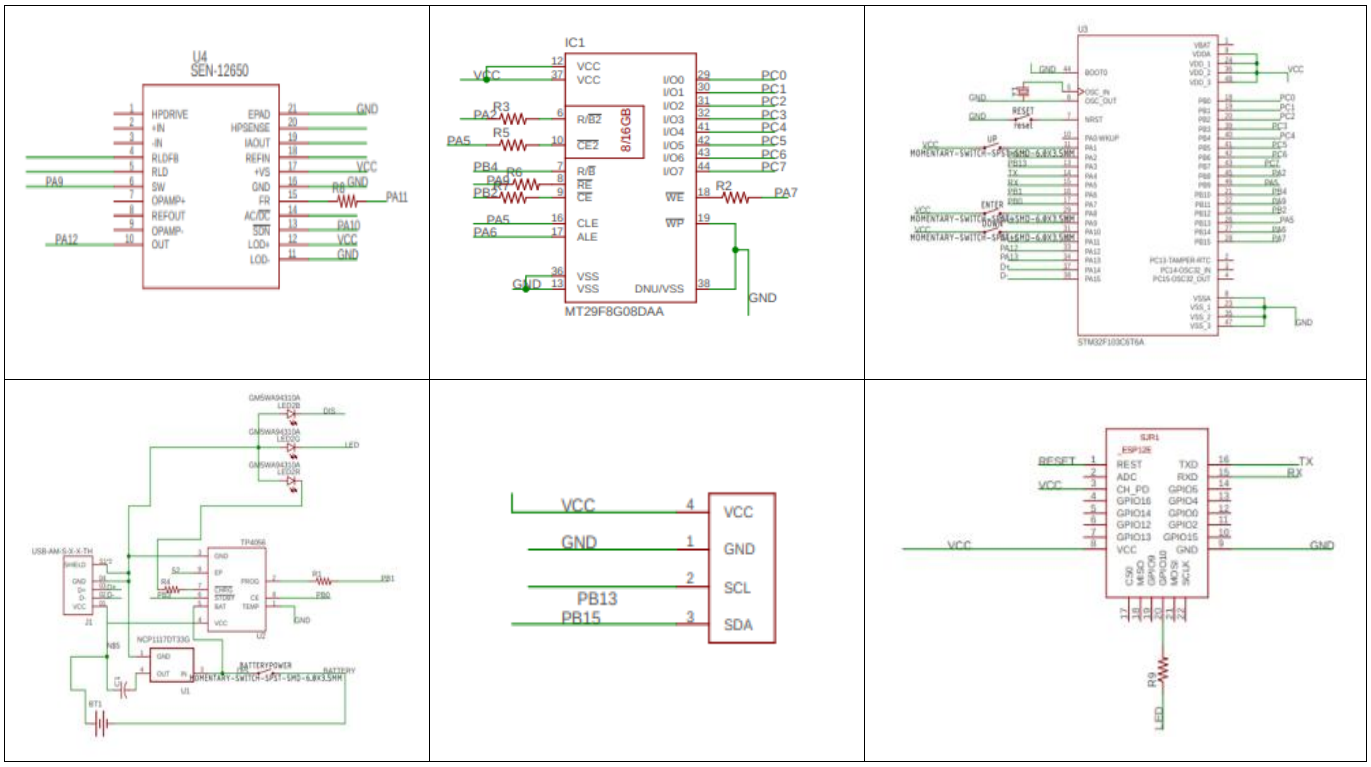
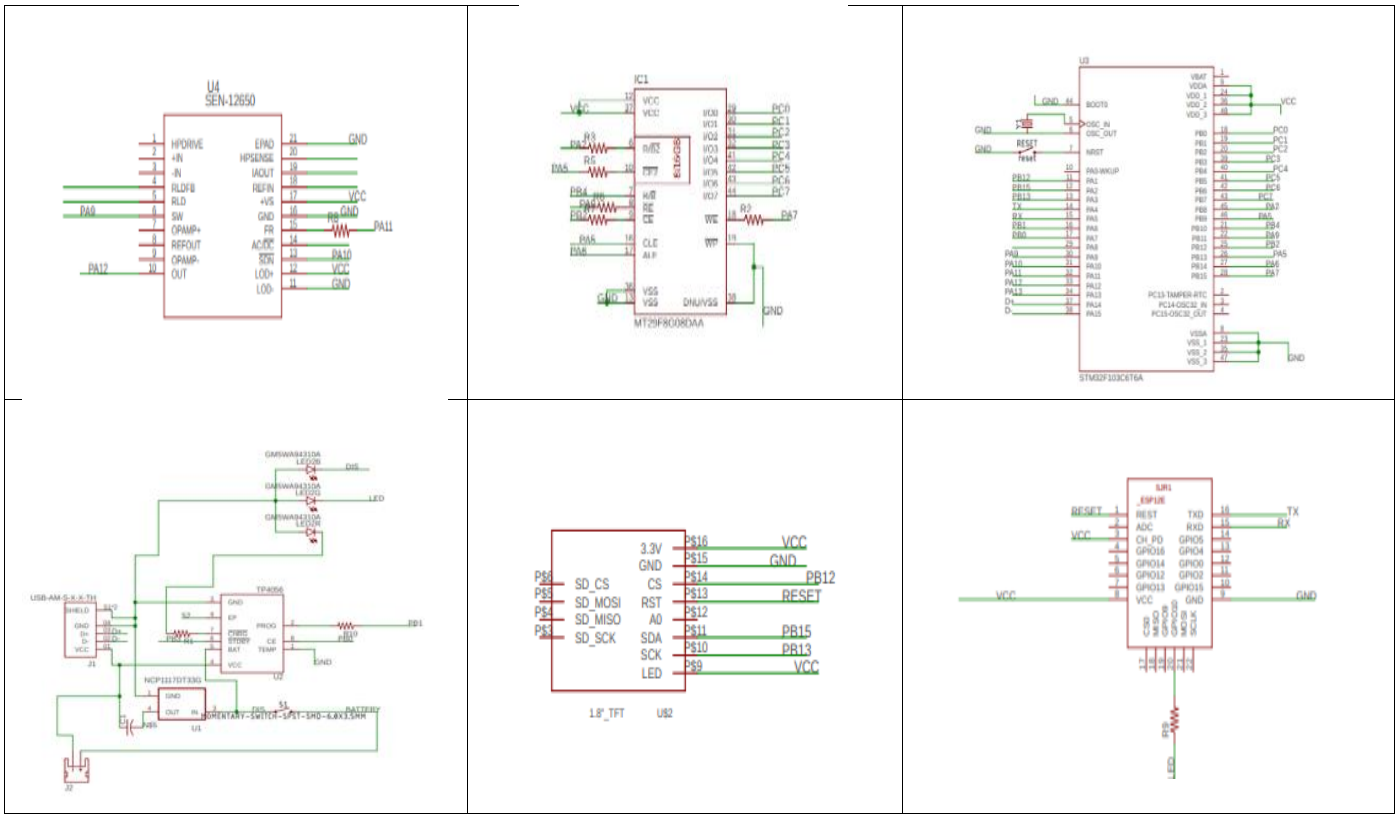


TABLE IV
THE DESIGNED SYSTEM SCHEMATIC II



The PCB and physical designs of the system reflect a balance between advanced features, user accessibility, and manufacturability. The dual-variant approach supports two distinct usage styles, and both designs provide space-efficient and robust housing for the project's embedded device. Images in Table IV, Figure 5 and 6 show the system engineering schematics, board and prototype

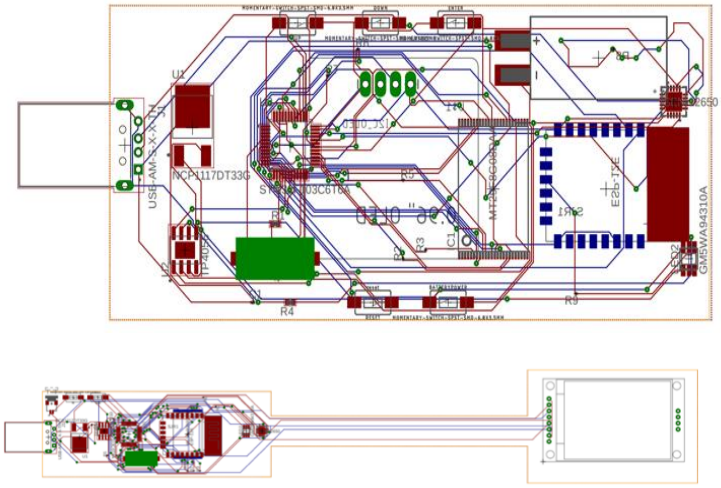


Figure 5. The designed system PCB

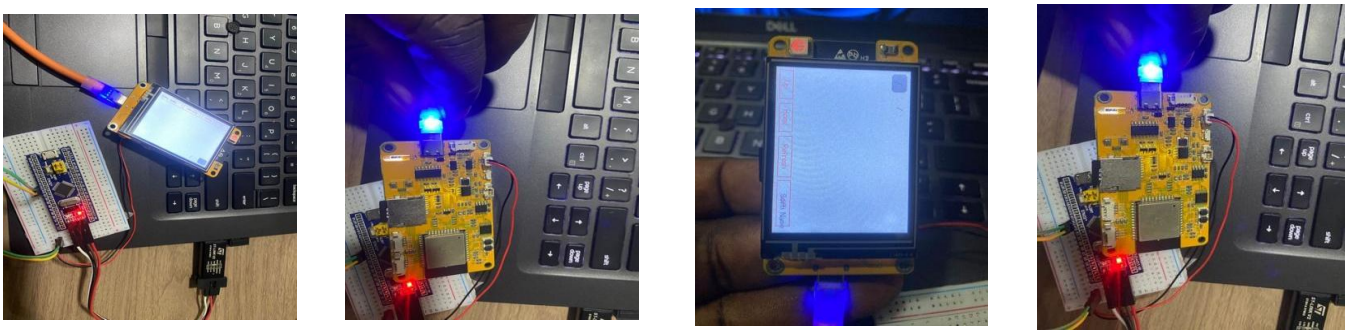


Figure 6. The build system prototype.

III. Result and Discussion

Below are the test environment indicating and hardware and software configurations, the functional test results, performance metrics, and the scalability testing.

- *Hardware Configuration:* ESP32 Dev Module with UI, storage, and system control. STM32 Microcontroller as peripheral control. A TFT Display with Touch Controller, a SD Card Module, a USB, Power Supply with Battery subsystem disabled.
- *Software Configuration:* Arduino framework for ESP32 and STM32 firmware using HAL and I²C interface for TFT touch. A SPI interface for TFT display and SD card. A serial communication between MCUs with No MQTT or network stack.

TABLE V
Functional Test Result

Test Subsys	Key Metrics	Result	Status
System Boot	Power-on, cold reset, warm reset	All success	✓ Pass
Display & Touch	Init, detection, failure handling	All success	✓ Pass
SD Card Storage	Mount, list, read, hot removal	All success	✓ Pass
MCU Comm.	Role switching, arbitration, commands	100% success	✓ Pass

TABLE VI
PERFORMANCE METRICS

Operation	Average Time
UI screen refresh	< 50 ms
Touch response	< 30 ms
File list load	< 120 ms
Serial command round-trip	< 10 ms
Role switch latency	< 5 ms

TABLE VII
STABILITY TESTING

Long Runtime Test:	System operated continuously for 6+ hours with no watchdog resets, no memory leaks observed, and UI remained responsive.
Reset Endurance Test:	50+ consecutive resets with no file corruption and no display or touch lockups.

The designed system demonstrated reliable operation under a dynamic master-slave communication model, allowing both ESP32 and STM32 microcontrollers to assume control roles as required. The challenges encountered during development were primarily integration and architectural issues, not conceptual flaws. Through systematic debugging and code-driven design revisions, the system was stabilized and improved. The designed system architecture proved flexible, fault-tolerant, and scalable, validating the design choices made during development. These changes are fully reflected in the final ESP32 and STM32 codebases and represent a mature, production-ready embedded system design suitable for academic and practical deployment.

IV. CONCLUSIONS

This technical report details the ongoing development of a next-generation multipurpose pen drive, aimed at addressing growing demands for portable, secure, and intelligent data storage. The study seeks to overcome those limitations by creating a self-contained, smart USB storage device that users can operate wirelessly, securely, and independently. The device is powered by a rechargeable lithium-ion battery, allowing it to function without external power. Users can view and interact with the device via either a button-controlled OLED interface or a touchscreen TFT interface, depending on the selected physical model. The interface shows live information such as transfer progress, Wi-Fi status, and battery level, thereby offering a truly interactive and transparent storage experience. The implementation followed a modular methodology, with each subsystem developed, tested, and optimized independently. Detailed design calculations were conducted to determine power consumption, battery life, and thermal safety. PCB schematics and 3D enclosure models were completed for both versions of the device. The prototype is still under construction, but test demonstrated significant technical achievements and provides a clear roadmap toward full realization. The proposed system addresses emerging concerns around data security, device portability, user convenience, and thermal or power management in modern computing environments. This work has demonstrated that secure, intelligent, and user-friendly portable storage is not only feasible but necessary in the modern digital landscape.

REFERENCES

[1] K. Shimizu, Y. Li, and R. H. Deng, "Portable Data Encryption Device with Configurable Security Functionality and Method for File Encryption," *U.S. Patent* 9,049,010 B2, Mar. 3, 2015.

[2] S. Mahna and C. Sravan, "An Efficient Data Transmission by Using Modern USB Flash Drive," *Int. J. Multimedia and Ubiquitous Engineering*, vol. 9, no. 4, pp. 1–10, 2014.

[3] H. Kim, Y. Lee, and J. Park, "Vulnerability Analysis of Secure USB Flash Drives," *J. Information Security Research*, vol. 6, no. 2, pp. 115–128, 2008.

[4] Espressif Systems, *ESP32 Technical Reference Manual*, Version 4.1, Espressif Systems, 2020. [Online]. Available: **https://www.espressif.com**

[5] STMicroelectronics, *RM0008: Reference Manual for STM32F103xx Advanced ARM-based 32-bit MCUs*, Rev. 20, Nov. 2021. [Online]. Available: **https://www.st.com**

[6] E. Wirth, "Thermal Management in Embedded Systems," M.S. thesis, Dept. of Electrical Engineering, Univ. of Illinois, Urbana-Champaign, IL, USA, 2004.

[7] Espressif Systems, "ESP32-WROOM-32 Datasheet — Version 3.6," Espressif Systems, 2021.

[8] Espressif Systems, "ESP32-WROOM-32E and WROOM-32UE Datasheet, v1.9," Espressif Systems, May 2020.

[9] STMicroelectronics, "RM0008 — Reference Manual for STM32F103xx Advanced ARM-based 32-bit MCUs," Rev. 20, STMicroelectronics, 2021.

[10] National Institute of Standards and Technology (NIST), "FIPS 197 — Advanced Encryption Standard (AES)," Nov. 2001.

[11] USB Implementers Forum (USB-IF), "Universal Serial Bus Specification, Revision 2.0," USB-IF, Apr. 2000.

[12] USB Implementers Forum (USB-IF), "Mass Storage Class (MSC) — Specification Overview," USB-IF, 2003.

[13] TopPower Semiconductor, *TP4056: 1A Standalone Linear Li-Ion Battery Charger with Thermal Regulation*, Datasheet, 2018.

[14] Solomon Systech Ltd., *SSD1306 OLED/PLED Driver Controller*, Datasheet, 2016.

[15] Hangzhou Grow Technology Co., *R307 Optical Fingerprint Module User Manual*, 2019.

[16] K. Nohl, S. Krißler, and J. Lell, "BadUSB — On Accessories That Turn Evil," *Black Hat USA Conference Proceedings*, 2014.

[17] H. Liu, J. Chen, and S. Zhang, "USB-Powered Devices: A Survey of Side-Channel Threats and Mitigations," *IEEE Access*, vol. 9, pp. 145371–145384, 2021.

[18] O. Ettahri, A. Rida, and A. J. M. Trabelsi, "A Real-Time Thermal Monitoring System Intended for Embedded Applications," *Sensors*, vol. 20, no. 23, 2020.

[19] Y. Lee, S. Kim, and H. Park, "Thermal-Aware Design and Management of Embedded Systems," in *Proc. Design, Automation & Test in Europe (DATE)*, 2021, pp. 1119–1124.

[20] M. Nicho, P. Obaid, and D. M. Zuckerman, "Bypassing Multiple Security Layers Using Malicious USB Devices," in *Proc. Int. Conf. Information Systems Security and Privacy (ICISSP)*, 2023.

[21] H. Jeong, J. Park, and Y. Lee, "Vulnerability Analysis of Secure USB Flash Drives," *J. Information Security Research*, vol. 6, no. 2, pp. 115–128, 2007.

[22] S. Malik and R. Patel, "BadUSB: The Threat Hidden in Ordinary Objects — A Comprehensive Survey," in *Proc. IEEE Conf. Cybersecurity and Privacy*, 2022