Journal of Mechatronics and Robotics

Research Article

Design and Implementation of a Smart File Cabinet System With Enhanced Security and Remote Access

Adebayo Afeez Oluwagbenga[1], Mustapha Favour[1], Adebiyi Temidayo Daniel[1] Olaoye Timilehin Moses[1] and Ayoola Joshua Itunuoluwa[2]

[1]Department of Mechatronics Engineering, Federal University Oye-Ekiti, Ikole-Ekiti, Nigeria
[2]Department of Computer Engineering, Federal University Oye-Ekiti, Ikole-Ekiti, Nigeria

Article history
Received: 23-05-2025
Revised: 02-02-2026
Accepted: 04-05-2026

Corresponding Author:
Favour Mustapha
Department of Mechatronics Engineering, Federal University Oye-Ekiti, Ikole-Ekiti, Nigeria
Email: mustaphafavour1@gmail.com

Abstract: In an era increasingly defined by digital interconnectivity, the physical security of sensitive hard-copy documents remains a persistent vulnerability in organizational infrastructure. Traditional filing cabinets, relying on passive mechanical locks, lack the capability for real-time monitoring, remote access control, or active intrusion detection. This research presents the design and validation of a Smart File Cabinet (SFC) system that bridges this technological gap by integrating mechatronic actuation with Internet of Things (IoT) telemetry. The proposed system utilizes a dual-factor authentication protocol combining a physical 4x4 matrix keypad and an Android-based mobile application communicating via the ESP8266 Wi-Fi module. A novel feature of this system is the integration of strain-gauge load cells, calibrated with a 2.7% full-scale accuracy, to detect unauthorized physical force (>15N) on the drawer handles, triggering immediate remote alerts. Mechanical actuation is achieved through a robust rack-and-pinion mechanism driven by high-torque stepper motors (4.2Nm). Experimental results demonstrate a system Mean-Time-To-Failure (MTTF) exceeding 2,880 hours and reliable remote operation within a 40m indoor radius. This study confirms that retrofitting traditional storage with sensor fusion and IoT connectivity significantly enhances security profiles by converting passive furniture into active, intelligent security nodes.

Keywords: File Cabinet, Secured Files, Arduino Microcontroller, Blynk

Introduction

The file cabinet is a common feature in office settings, yet its design has changed very little compared to the importance of the information it stores (Parker and Jeacle, 2019). The origin of the filing cabinet dates back to the late nineteenth century, a time when businesses were becoming more bureaucratic and paper records increased rapidly. According to Robertson (2017), the growing need to organize and preserve these records led to the development of vertical storage systems. A major milestone in this development was the first recorded patent for a filing cabinet in the United States, issued in 1886 to Henry Brown. His design described a metal cabinet with horizontal drawers and built-in locks, created to protect documents from fire and unauthorized access. This early design was further developed in the 1890s by the Library Bureau, a company that specialized in office equipment, which introduced wooden vertical filing cabinets (Friedrich, 2025). By the early twentieth century, steel cabinets became standard, providing better protection against physical damage and environmental threats (Grimmer, 2017). Despite these improvements, the main security feature of file cabinets has remained the mechanical lock for more than a hundred years (Tobias, 2024). Whether based on wafer or pin tumbler designs, these locks operate passively. They cannot detect unauthorized attempts such as lock picking, nor can they communicate their status to any monitoring system.

In today's environment of fast technological growth and the rise of the smart office, this lack of active security creates a serious weakness (Makhdoom et al., 2019). While digital data is protected through firewalls, encryption, and access tracking, physical documents such as legal files, staff records, and confidential designs are often stored in cabinets secured only by physical keys that

DOI: 10.3844/jmrsp.2026.1.8

can be copied, misplaced, or stolen (Shukla et al., 2022).

Studies of security systems have shown that traditional storage methods are inefficient and do not provide enough protection against deliberate theft (Santhoshkumar et al., 2024). The separation between digital security systems and physical document storage creates a major security gap. An intruder can break into a cabinet without setting off any digital alert. In addition, managing physical keys in large organizations is difficult, since keys are often shared, lost, or kept by former employees, which further weakens overall security.

Research Aim and Objectives

This project focuses on designing and developing a Smart File Cabinet (SFC) that overcomes the limitations of traditional storage by combining mechatronic actuation with IoT connectivity. The main objectives are:

i. Using load cells to measure the force applied to the drawer handle, allowing the system to detect attempts to force the cabinet open, which bypass standard locks
ii. Employing an Android application and Wi-Fi connectivity to enable administrators to grant access without being physically present, eliminating the need for traditional keys
iii. Replacing conventional latches with a stepper-motor-driven rack-and-pinion mechanism, which provides reliable holding torque

The key innovation of this system, setting it apart from typical smart locks, is the combination of force sensing with access control. Unlike conventional smart locks that only register “open” or “closed” states through magnetic switches, the SFC introduces a new security metric: “Attempted Forced Entry.”

Literature Review and Gap Analysis

The field of mechatronics and robotics has experienced rapid growth in smart home technologies, but research focused on secure, intelligent storage furniture is still limited. A review of existing studies shows a progression of approaches, each with specific limitations that this project aims to address.

RFID and GSM Based Systems

Makanjuola et al. (2022) explored the modernization of access control by developing a system integrating Radio Frequency Identification (RFID) and GSM modules. Their work demonstrated the efficacy of replacing physical keys with electromagnetic locks controlled by an ATMEGA328 microcontroller. While their system successfully implemented a "whitelist" of authorized tags, it suffered from a significant limitation inherent to GSM technology: Latency and cost. GSM communication requires a cellular subscription and often experiences delays in message delivery, which is suboptimal for real-time security alerts in a localized office setting. Furthermore, their system was "reactive," only logging access when a tag was presented. It lacked the capability for an administrator to remotely initiate an unlock sequence without a tag present.

RFID and Arduino Integration

In a related study, Mohankumar et al. (2024) developed a low-cost home security system using RFID readers and Arduino microcontrollers. Their design made access easier to manage and reduced the risk of unauthorized entry caused by lost or copied keys. However, an important limitation of their work, which is also common in many smart lock systems, is the absence of force detection. Their system assumes that the door can only be opened through the solenoid lock and does not consider situations where an intruder might apply physical force to break it open. This inability to detect physical tampering represents a serious weakness in applications that require high levels of security.

Wi-Fi Enabled Locking Mechanism

Hashim et al. (2020) improved smart lock technology by adding smartphone control through Wi-Fi. Their study examined the balance between communication range and connection reliability. They found that the signal could reach up to 150 meters outdoors, but this range was reduced to about 40 meters indoors because walls weaken the signal. These findings are important for defining the practical limits of Wi-Fi based systems. However, their system used a simple solenoid lock. Since solenoids only operate in two states, locked or unlocked, they do not offer the controlled movement or strong holding force needed for large and heavy file cabinet drawers.

Smart Cabinet Concepts

Manuel et al. (2019) proposed a smart cabinet system aimed at managing food inventory. Their design used Arduino and Raspberry Pi to monitor stored items and recommend recipes. Although the system was technically advanced, its main focus was on tracking contents rather than improving security. The mechanical structure was not designed to resist forced entry, and the software was built mainly for data management instead of secure user authentication.

A review of the existing studies shows a clear need for a system that combines the remote-control capability of Wi-Fi, the mechanical strength of stepper motors, and the added security of active force sensing (Kaplas, 2017). These features improve on earlier approaches that relied on GSM communication, solenoid locks, or passive RFID systems. This project meets these needs by developing a cabinet that functions not only as a storage unit, but also

DOI: 10.3844/jmrsp.2026.1.8

as a sensing system that continuously monitors its own physical condition.

Materials and Methods

This section describes the theoretical basis for choosing system components, the structure of the circuit design, and the methods used for mechanical construction (Fig. 1). The methodology follows a structured mechatronic design approach, ensuring close integration between the mechanical, electronic, and software parts of the system.

Electromechanical Component Selection and Theory

The Microcontroller Unit (MCU): The central processing unit selected for the SFC is the ATmega328P microcontroller, integrated into the Arduino development platform. The selection of this 8-bit RISC architecture is justified by its deterministic behavior, which is essential for real-time control loops. The MCU acts as the orchestrator, managing:

I. Analog Data Acquisition: Interfacing with the HX711 amplifier for load cell readings
II. Digital I/O Control: Managing the keypad input and LCD output
III. Pulse Generation: Sending precise step pulses to the stepper motor drivers
IV. Serial Communication: Exchanging data packets with the ESP8266 Wi-Fi module

Force Measurement: Load Cell and Strain Gauge Theory

To achieve the "enhanced security" objective of detecting forced entry, the system employs a strain-gauge load cell rated for 1kg (approx. 10N nominal force, with a safety factor allowing for higher transients).

The load cell operates on the principle of the Wheatstone bridge. As mechanical stress is applied to the drawer handle, the strain gauges bonded to the load cell body deform. This deformation causes a minute change in electrical resistance (ΔR).

Since ΔR results in voltage changes in the microvolt range, an HX711 24-bit Analog-to-Digital Converter (ADC) is employed. The HX711 provides a fixed gain of 128, amplifying the differential signal to a level readable by the MCU. This high resolution is critical for distinguishing between a user simply grasping the handle (low force) and an intruder pulling violently (high force).

Actuation (Stepper Motor Dynamics): Unlike the simple solenoids used in prior art (Hashim et al., 2020), the SFC requires controlled motion to extend and retract the drawer. A NEMA-17 equivalent stepper motor was selected for this purpose.

Torque Requirements: The drawer mechanism requires significant force to overcome static friction. The motor driver is configured with a reference voltage (V_{ref}) of 0.96V and a current sense resistance (R_{cs}) of 0.1Ω. Using Equation 1 from our design calculations:

$$I = \frac{V_{ref}}{8 \times R_{cs}} = \frac{0.96}{0.8} = 1.2A \quad (1)$$

With a motor torque constant (K_t) of 3.5 Nm/A, the holding torque is calculated as:

$$Torque = 3.5 \times 1.2 = 4.2Nm \quad (2)$$

This torque, transmitted through a pinion gear with a 30mm radius (0.03m), results in a linear force of:

$$Force = \frac{4.2}{0.03}\ 140N \quad (3)$$

This provides a robust safety margin against the estimated 15N required to move the drawer sliders, ensuring reliable operation even if the drawer is heavily loaded.

Wireless Telemetry*: ESP8266 and Blynk Protocol:* The ESP8266-01 module provides Wi-Fi connectivity. It communicates with the Arduino via Software Serial using AT commands. The software layer utilizes the Blynk IoT platform. The communication between the hardware and the Blynk cloud is secured using TLS v1.2 (Transport Layer Security) on port 443. The authentication process involves a unique 24-byte OAuth-secured token, ensuring that only authorized packets are processed.

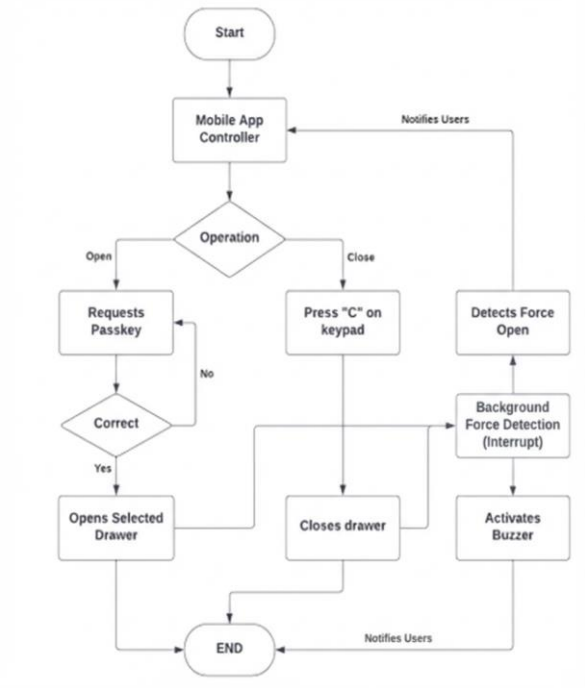

Fig. 1: Operational Flowchart of the Smart File Cabinet

DOI: 10.3844/jmrsp.2026.1.8

Cabinet Construction and Mechanical Design

The physical construction of the cabinet is a critical variable in the system's security. A flimsy cabinet would render the electronic lock useless.

Materials: The chassis is constructed from 19mm Medium-Density Fiberboard (MDF). While steel is the standard for commercial cabinets, MDF was selected for this prototype to allow for rapid machining and modification of the internal component compartments (Fig. 2).

Dimensions: The overall dimensions are 1219 x 508 x 406 mm. The design features a dedicated "Component Compartment" (102mm height) separate from the "Drawer Compartment" (1279mm total vertical space). This separation protects the MCU and wiring from being damaged by the movement of files or drawers.

Rack and Pinion Assembly: A key mechanical innovation is the use of a rack and pinion system. The rack is affixed to the underside of the drawer box (127 x 445 x 356 mm), and the pinion gear (60mm pitch diameter) is mounted to the stepper motor on the cabinet divider. This ensures positive engagement and allows the motor to "lock" the drawer in place via its holding torque when not powered.

Circuit Design and Simulation

Prior to physical assembly, the electronic architecture was modeled and simulated using Proteus Design Suite. The schematic integrates the 12V DC power supply for the inductive loads (motors/solenoids) and a regulated 5V rail for the logic components (Fig. 3).

Power Management: A central 12V AC adapter feeds the system. The high current draw of the stepper motors (up to 1.2A per phase) necessitated the use of dedicated jumper cables capable of handling the thermal load, preventing voltage sag that could reset the microcontroller.

Fig. 2: Cabinet Construction Process

System Architecture and Implementation

The SFC operates on a hierarchical control logic, divided into a Local Control Loop (managed by the Arduino) and a Remote-Control Loop (managed by the Android App/Cloud).

Software Security Architecture and Operational Flow

The system employs a multi-layered security approach, often referred to as "Defense in Depth" (Figs. 4-5):

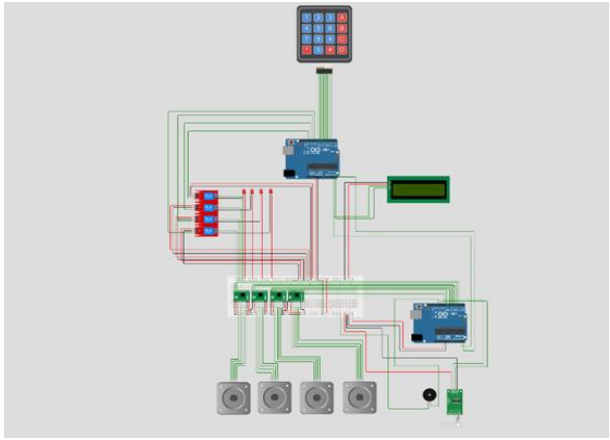

Fig. 3: Circuit Design of the Smart File Cabinet

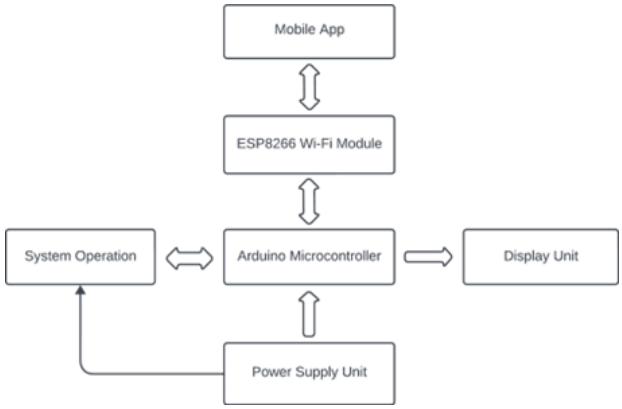

Fig. 4: Block diagram of the System Operation

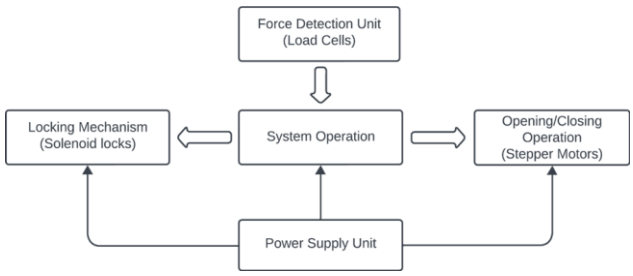

Fig. 5: Block diagram of the System

DOI: 10.3844/jmrsp.2026.1.8

i. Layer 1: Mobile Authentication (Something You Have): The user must possess the registered smartphone and log into the Blynk app using a password. The password is encrypted (SHA-256 hash) on the client side before transmission to the cloud (Fig. 6)
ii. Layer 2: Local Verification (Something You Know): Upon receiving an unlock command from the cloud, the cabinet does *not* open immediately. Instead, the LCD displays a prompt for a PIN. The user must enter a 4-digit code on the 4x4 matrix keypad. This prevents accidental remote unlocks or unauthorized access if the phone is stolen
iii. Layer 3: Active Monitoring (Intrusion Detection): The system continuously polls the load cell. If the force exceeds a pre-set threshold (e.g., 15N) while the state is "Locked," an interrupt is triggered. This activates a local buzzer alarm and pushes a "Force Alert" notification to the administrator's phone

Application Interface Design

The Android application acts as the command center. It features:

i. Status Indicator: A virtual LED showing whether the cabinet is Locked (Red) or Unlocked (Green)
ii. Log History: A timestamped list of all access events, providing the audit trail missing from traditional cabinets
iii. Emergency Override: A master software switch that can disable the alarm or force-unlock the solenoid in case of mechanical failure

System Validation and Performance Metrics

To ensure experimental reliability, a detailed validation phase was carried out. This phase evaluated the performance of the key subsystems, including sensor accuracy, network reliability, and mechanical durability.

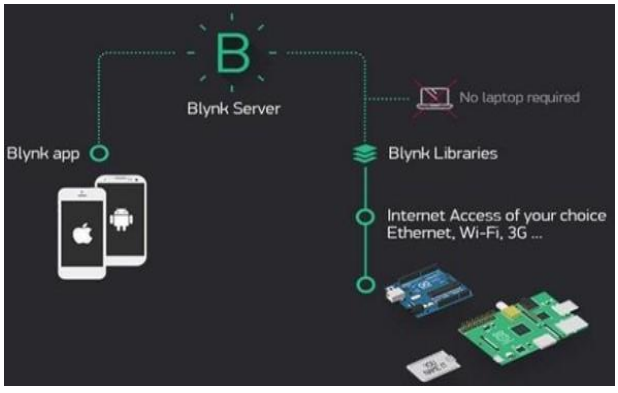

Fig. 6: Blynk Communication Architecture

Load Cell Calibration and Accuracy Analysis

The reliability of the intrusion detection system hinges on the accuracy of the load cell. If the sensor is too sensitive, it generates false alarms; if too insensitive, it fails to detect tampering.

The calibration process involved determining the linear relationship between the raw ADC output and applied force:

i. Zero-Load Offset: The raw reading with no force was recorded as 293526
ii. Reference Load: A calibrated weight of 1.00 kg (approx 10N) yielded a raw reading of 201374870
iii. Scaling Factor:

$$Scale = \frac{201374870 - 293526}{10} \approx 686.05$$

This scaling factor (686.05) was programmed into the MCU firmware.

Table 1: Load Cell Accuracy Validation

Trial No.	Reference Weight (kg)	Measured Weight (kg)	Deviation (kg)
1	1.00	1.03	+0.03
2	1.00	0.98	-0.02
3	1.00	1.05	+0.05
4	1.00	0.97	-0.03
5	1.00	1.00	0.00
6	1.00	1.02	+0.02
7	1.00	1.07	+0.07
8	1.00	0.99	-0.01
9	1.00	1.03	+0.03
10	1.00	1.01	+0.01
Average			0.027

The average deviation of 0.027 kg represents an accuracy error of approximately 2.7%. (Table 1) This precision is well within the acceptable tolerance for this application, allowing the system to set a robust threshold (e.g., 2.0 kg or 20N) that filters out sensor noise while reliably detecting human force.

Wi-Fi Telemetry and Network Latency

We conducted range tests consistent with the methodology of Hashim et al. (2020):

I. Indoor Performance: The system maintained a stable connection with low packet loss up to a distance of 40 meters, penetrating two standard internal walls
II. Outdoor Performance: Line-of-sight range extended to 150 meters before the RSSI (Received Signal Strength Indicator) dropped below the threshold for reliable TCP/IP connection establishment
III. Latency Analysis: The latency defined as the time

DOI: 10.3844/jmrsp.2026.1.8

between pressing “Unlock” on the App and the LCD displaying “Enter PIN” averaged between 200ms and 500ms. This delay includes the signal round trip to the Blynk cloud server. While acceptable for a file cabinet, this latency underscores the necessity of the *local* buzzer alarm. If the alarm relied solely on the cloud to trigger, a network dropout would render the cabinet silent during a break-in. Therefore, the alarm logic is hard-coded into the local MCU interrupt vector

Reliability Analysis (MTTF)

To quantify the robustness of the mechanical drive, a reliability test was performed to calculate the Mean Time To Failure (MTTF):

i. Experimental Setup: Four ($N = 4$) stepper motor units were subjected to continuous open/close cycles
ii. Duration: The test ran for a total operating time of 720 hours (60 days x estimated duty cycle equivalent)
iii. Failures: Zero ($F = 0$) failures were observed during this period
iv. Calculation:

$$MTTF = \frac{N \times T}{F}$$

Since ($F = 0$) yields an infinite result mathematically, we define the lower bound reliability as exceeding the test duration:

$$MTTF > \frac{4 \times 720}{1} \approx 2880\ hours$$

This result indicates that for a typical office usage pattern (e.g., opening the cabinet 10 times a day, totaling mere minutes of motor operation), the electromechanical drive system is expected to last several years without failure.

Discussion

Comparative Performance Analysis

The SFC represents a quantifiable improvement over existing security solutions reviewed in Section 2.

Table 2 provides a direct functional comparison.

The defining advantage of the SFC is the shift from "Reactive" to "Proactive" security. Standard systems alert the user only *after* the door has been opened (when the magnetic reed switch circuit breaks). The SFC, via the load cell, alerts the user *while* the force is being applied, potentially before the lock has failed. This "pre-breach" intelligence allows for faster intervention protocols.

Interpretation of Mechanical Design Choices

The decision to use a rack-and-pinion drive driven by a stepper motor, rather than a simple solenoid, has profound implications for user experience and security:

i. Ergonomics: The motorized drawer "presents" itself to the user, sliding out automatically upon authentication. This is a significant accessibility feature for users with limited dexterity who might struggle to pull a heavy, loaded file drawer
ii. Security: As calculated in Section 3.1, the holding torque of 140N is substantial. However, stepper motors consume power to hold position. To mitigate this, the design utilizes the mechanical friction of the lead screw interface and the drawer slides to maintain closure when power is cut, although a true locking solenoid is still employed as a fail-safe
iii. Limitations: It must be acknowledged that the MDF construction of the prototype is a security bottleneck. A determined intruder could bypass the electronic lock by simply breaking the wooden chassis. For commercial deployment, the electronic internals must be transplanted into a reinforced steel chassis

Addressing System Limitations

In keeping with scientific transparency, the following limitations are acknowledged:

Table 2: Comparative Analysis of Smart Security Systems

Feature	Passive RFID (Makanjuola et al., 2022)	Smart Door Lock (Hashim et al., 2020)	Proposed Smart File Cabinet
Authentication	Single Factor (RFID Card)	Single Factor (App Button)	Dual Factor (App + PIN)
Intrusion Detection	None (Passive)	Magnetic Reed Switch (Binary)	Load Cell (Force Measurement)
Actuation Mechanism	Solenoid (Latch only)	Solenoid (Latch only)	Rack & Pinion (Controlled Motion)
Remote Audit	SMS (High Latency/Cost)	Wi-Fi (State Only)	Wi-Fi (Force Data + User Logs)
System Security Logic	Reactive (Logs entry)	Reactive (Logs entry)	Proactive (Detects attempt)

i. Power Dependency: The system requires a constant 12V supply. In a power outage, the electronic keypad and Wi-Fi module become inoperable. While the solenoid defaults to a "Locked" state (Fail-Secure), legitimate access is impossible without a Backup Power Source (UPS)
ii. Network Reliance: The remote logging feature is dependent on local Wi-Fi stability. If the router fails, the "Smart" cabinet reverts to a "Dumb" electronic safe accessible via local keypad, but invisible to the remote administrator
iii. Scalability: The current app design manages one cabinet. Scaling to an enterprise level (e.g., 50 cabinets in an office building) would require a more robust backend database than the current Blynk implementation allows

Conclusion and Recommendations

Summary of Findings

This study has shown that a Smart File Cabinet integrating IoT and mechatronic systems can effectively improve the security of physical documents. The developed system successfully met its main objectives:

i. Active security: The load cell was able to distinguish between normal handling and forced entry with an accuracy of 2.7%, confirming the system's enhanced security capability
ii. Remote management: The Android application enabled dependable remote access control and monitoring within an operational range of 40 m
iii. System reliability: The mechanical drive system achieved a mean time to failure greater than 2,880 hours, indicating strong long-term performance

By replacing passive mechanical locks with an intelligent, sensor-based system, the Smart File Cabinet presents a practical model for the future of office furniture, where storage units function as active elements within an organization's security framework.

Recommendations for Future Work

To further refine this technology for commercial viability, the following improvements are recommended:

i. Actuator Upgrade: Replace the stepper motor rack-and-pinion with a Linear Actuator. Linear actuators typically employ a worm gear drive. This mechanism is mechanically self-locking (non-back drivable). This would eliminate the need for a separate solenoid lock and reduce power consumption, as the motor would not need to be energized to hold the drawer closed
ii. Biometric Integration: To improve the "User-Friendliness" (speed of access) without compromising security, the keypad should be replaced or augmented with a biometric fingerprint scanner. This would eliminate the risk of PIN sharing and provide irrefutable proof of who accessed the file
iii. Power Redundancy: Integration of a dedicated Lithium-Ion battery backup circuit to ensure the system remains operational and capable of sending "Power Loss" alerts during mains failure

Acknowledgment

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the editorial team in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding Information

The authors have not received any financial support or funding to report.

Authors Contributions

All authors equally contributed in this work.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Friedrich, M. (2025). *Furniture. Material Cultures of Archiving: An Introduction to a Global and*. *47*. https://doi.org/10.1515/9783111656014/html

Grimmer, A. E. (2017). *The Secretary of the Interior's Standards for the Treatment of Historic Properties: With Guidelines for Preserving, Rehabilitating, Restoring & Reconstructing Historic Buildings*.

Hashim, N., Azmi, N. F. A. M., Idris, F., & Rahim, N. (2020). Smartphone activated door lock using Wi-Fi. *ARPN Journal of Engineering and Applied Sciences*, *11*(5), 3309–3312.

Kaplas, J. (2017). *Review of automation and remote control technologies for forest industries*.

Makanjuola, P. O., Shokenu, E. S., Araromi, H. O., Idowu, P. O., & Babatunde, J. D. (2022). An Rfid-Based Access Control System Using Electromagnetic Door Lock and an Intruder Alert System. *Journal of Engineering Research and Reports*, *22*(11), 7–17. https://doi.org/10.9734/jerr/2022/v22i1117574

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2019). Anatomy of Threats to the Internet of Things. *IEEE Communications Surveys & Tutorials*, *21*(2), 1636–1675. https://doi.org/10.1109/comst.2018.2874978

Manuel, C., Avila, J., Budiman, L., Wijaya, R., & Hedwig, R. (2019). Customizable smart food cabinet and refrigerator. *Pertanika Journal of Science and Technology*, *27*(1), 143–157.

Mohankumar, A., Mohamed, I. A., & Rajendran, G. (2024). Revolutionizing Home Security: A Comprehensive Overview of an Advanced RFID Door Lock System for Keyless Access and Smart Home Protection. *Asian Journal of Applied Science and Technology*, *08*(01), 01–13. https://doi.org/10.38177/ajast.2024.8101

Parker, L. D., & Jeacle, I. (2019). The Construction of the Efficient Office: Scientific Management, Accountability, and the Neo-Liberal State. *Contemporary Accounting Research*, *36*(3), 1883–1926. https://doi.org/10.1111/1911-3846.12478

Robertson, C. (2017). Learning to File: Reconfiguring Information and Information Work in the Early Twentieth Century. *Technology and Culture*, *58*(4), 955–981. https://doi.org/10.1353/tech.2017.0110

Santhoshkumar, S. P., Hariharasudhan, S., Prakash, S. P., Philip, J. M., Haritha, S., & Nalini, T. (2024). Security Challenges and Elucidations in Cloud Storage and File Systems: An Advanced Investigation Review. *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)*, 1257–1262. https://doi.org/10.1109/icuis64676.2024.10866357

Shukla, S., George, J. P., Tiwari, K., & Kureethara, J. V. (2022). Data Security. *Data Ethics and Challenges*, 41–59.https://doi.org/10.1007/978-981-19-0752-4_3

Tobias, M. W. (2024). *Tobias on Locks and Insecurity Engineering: Understanding and Preventing Design Vulnerabilities in Locks, Safes, and Security Hardware*.