International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(21s) 2026 pp. 773-792
https://doi.org/10.70917/ijcisim-2026-5343
Article

An Energy Efficient Multi Finger Biometric Digital Locker for Safeguarding Physical Files: Design, Security Evaluation and Power Modelling

Venkappanavara Basavaraja[1], Yathish N A[2], Chandrakant Naikodi[3]

[1]Research Scholar,Department of Studies in Computer Science,Davangere University- 577007 India Email: v.basavaraja@gmail.com
[2]Research Scholar,Department of Studies in Computer Science,Davangere University- 577007 India Email: yateeshna@gmail.com
[3]Professor, Department of Studies in Computer Science, Davangere University- 577007 India
Email: chandrakant.naikodi@yahoo.in
Corresponding author:- Venkappanavara Basavaraja
Email:- v.basavaraja@gmail.com

Abstract: Even when digital document systems have been implemented, physical files are still necessary in offices, educational institutions, banks, archives, and legal settings. The main problem of relying on paper files is that they can be lost or stolen. However, digital lockers are insecure since they are based on conventional means of security that can be lost, shared, seen, duplicated, circumvented, or bypassed. This work describes a secure digital locker system for protecting physical files that integrates Internet of Things, biometrics, and four sensor systems, and includes an energy efficient management system. The proposed system contains a file latching and locking system, four fingerprint pods, a low power control module, a display module, a tamper evidence system, and an internal locking and latching system that opens after meeting the configured authentication requirement. The construction and offered simulations of the system are used to evaluate three domains of performance; the discrimination capacity of the biometrics, the system's energy use and efficiency, and the security provided by the system in relation to the most common attacks, both physical and logical. The four sensor system design achieves an overall sample equal error rate of 3.94 % at the 0.50 threshold, while the energy management system in the design decreased power consumption during the authentication process by 74 %. A 12.2 Wh lithium ion cell battery model estimates 2.8 years of potential operation with an approximate average of twenty unlocks per day. The study shows that the proposed system offers a valuable moderate solution for balancing robust file access control with the ability for long periods of operation. However, extensive user trials, liveness tests, and environmental stress tests must be conducted before this system can be deployed in an institution.
Keywords: biometric authentication, digital locker, physical file security, Internet of Things, fingerprint sensor, false acceptance rate, false rejection rate, energy efficiency, tamper detection

1. Introduction

The demise of non-digital records has been greatly exaggerated. Real, signed documents, for example, land deeds, court records, bonds, certificates, consent forms, and registers, maintain legal and administrative integrity well beyond the utility of their digitally recorded and retrieved copies. Well-managed digital systems speed document access, but the original signed document is often the artifact of ultimate trust. Stronger design systems for the protection of physically stored documents is therefore warranted. Document safes and file cabinets that appear

mundane may in fact contain documents that determine ownership, identity, employment, compliance, and accountability. The risks of document safety are concrete, and the void of a document can delay the resolution of a legal case, breach the privacy of a document, undermine the legitimacy of an administrative process, or facilitate the perpetration of fraud. My purpose is to address this reality, rather than a model of access control, that is solely theoretical.

Mechanical keys, numeric locks, shared office custody, and sometimes, electronic access devices are still the dominant systems in securing file cabinets and document boxes. While convenient, systems based on locks and keys, or access codes, or even shared custody, can all have downsides. Keys can always be duplicated or lost. Codes can be shared or guessed. Shared custody can work in a small office, but can easily be subverted by higher staff turnover, informal access, and a lack of proper audits. A fingerprint reader can be an improvement in personal accountability, since it requires the user to present a biological trait. However, relying solely on one biometric can present the same challenges. It can restrict access for legitimate users if the system does not have the proper settings to allow access, and it can allow access for impostors if the system has inadequate protection against spoofing. In biometrics parlance, this is a tradeoff between false rejections and false acceptances that must be managed, and cannot be arbitrarily assorted to the system.

The proposed model addresses these weaknesses by integrating physical, biometric, and energy management approaches to file security. This is more sophisticated than simply attaching a fingerprint lock to a storage box. This is a digital storage system model in which a physical belt or locking structure encircles a bundle of files or a cabinet hasp, while four fingerprint sensors are placed at optimal locations. A microcontroller supervises the authentication process in conjunction with the display, lock, and event management. In this design, one of the sensors is in an active ready state, while the others are in a sleep or low power state. While this design choice is fairly minor in most applications, a file locker is expected to run for months or years without needing to be recharged. If, however, this design choice is poorly implemented, then the locker is defeated, because the security device itself is the most vulnerable part of the system due to battery drain.

In this paper, a digital locker is a cyber physical device designed to secure physical documents. This should not get conflated with document repository systems that save files in the cloud that are either scanned or issued in electronic format. These systems are useful, but they are designed to protect digital copies. The current model protects physical artefact with a hardware based locking system, local biometric authentication and power aware IoT control. The distinction is critical because a physical document that is a signed record or paper certificate can be stolen even if its digital copy are stored securely in some other location. The same can be said for a digital record of an audit log that is not physically controlled with a locking mechanism that protects it from unauthorised accesses and contains a control to log all access events.

Standards for authentication and frameworks for the testing of biometrics significantly contribute to the design. For instance, NIST SP 800 63B 4 defines authentication as ascertaining that the claimant is the subscriber who was previously authenticated. In contrast, ISO/IEC 19795 1 considers the empirical evaluation of biometric systems through error and throughput measures. NIST SP 800 76 2 and ISO/IEC 19794 2 are pertinent to this discussion as they cover specifications for fingerprints and minutiae representation. Although these standards do not design a physical file locker, they help structure the work. They indicate to the researcher that authentication is not an abstract assertion of security. It is to be measured, and reported, and is to have claimed limits with test conditions. Likewise, baseline guidance for IoT, such as NISTIR 8259A and ETSI EN 303 645, encourages the designer to address device identity, data protection, secure update, logging and configuration as primary design issues rather than mere afterthoughts.

The current study uses a progressive research design across prototype reports, a component level system description, an interactive simulation module, and biometric performance analyses and includes some of my earlier work. Previous research focused on the collection of literature and the development of methodologies. The intermediate work refined the architecture into a four sensor system, included performance analysis using false accept

and false reject rates, and extended the design into an explicit energy efficient model. The final version reorganizes the materials into a research article. In doing so, it adopts the constructively critical position of a researcher on the evidence. The performance data of the prototype and the threshold sweeps suggest that the design is promising, but cannot substitute for a complete field evaluation. A research article can and should take a position of positive assurance on what its data indicate, and assume a critical posture on what still needs to be measured.

The core research question is simple: can the design of a multi-finger biometric digital locker strike a balance of improving the control of access to physical files and maintaining an energy profile that supports its operation over long periods of time without user interaction? The design of such a locker brings with it the question of how, and with what level of assurance, the claims of security and energy efficiency can be evaluated. This paper attempts to answer this question with an outline of the architecture, performance metrics of the biometric system, power modeling, a security threat analysis, and a review of the current literature on IoT lockers and biometric authentication.

The contribution of the study lies in the integration rather than one isolated component. Fingerprint sensors are not new. Microcontrollers are not new. Servo motors, OLED displays and IoT communication are not new. The contribution is the way these elements are arranged around the specific problem of protecting physical files: multiple fingerprint points, sequential sensor wake scheduling, local template storage, tamper aware belt design, a physical latch and a measurable energy model. This arrangement provides a practical direction for institutions that need stronger protection than a key based file cabinet but cannot afford a complex, permanently powered security enclosure.

2. Literature Review

Biometric authentication has served as a third category of access control methods, along with knowledge and possession-based methods. According to the traditional description, a password is based on the user's knowledge, a key or token is based on the user's possession, and biometric verification is based on who the user is or what the user does. Jain, Ross, and Prabhakar (2004) formalized this distinction and attributed problems of biometric recognition to pattern recognition problems involving acquisition, feature extraction, matching, and decision. This distinction is foundational and important because it states that a biometric system is not a sophisticated identity oracle; rather, it is only a quality sensor that is subject to a variety of factors involved in the sensing, the enrollment, the environment, the user, and the aging of the template, and the thresholds.

Authentication literature describes the same idea in regard to the access control problem. Velasquez and co-authors examined authentication methods and classified them according to context, risk, and usability. Arias Cabarcos, and co-authors, advanced the discussion and presented the concept of adaptive authentication. The same applies to the context of access control. A biometric locking system in the home, fingerprint unlocking in a mobile phone, and a locking system for documents in an office, represent different models of access control. The design of a file locking system for restricted user groups, sensitive documents, and need for physical protection against forced access accommodates this understanding.

The advent of IoT has brought a variety of different lockers and components, including: RFID, PINs, OTPs, facial recognition, smartphones, fingerprint sensors, cloud storage, and even blockchain. The rapidly growing literature on smart lockers reflects this trend. One of the more recent smart lockers, developed by Alzhrani et al. (2024), incorporates the Internet of Things and a variety of access control measures, including: phone number verification, OTP, facial recognition, fingerprint, and emergency code. This type of solution can be very effective for the lock-out dilemma, since users can choose a more favorable security solution. However, there are likely to be problems with user accessibility, and the models may require more extensive network access to control locker activities.

There has also been work on decentralized storage and digital lockers with a focus on the integration of blockchain technology. Singhal et al. (2022) developed the DD Locker, a personal digital document storage solution built on the principles of blockchain. Many concepts associated with this solution have been developed in the context of digital storage and have focused on the integrity and auditability of digital documents. Some of the documents,

however, may require the user to physically control the release of a document. Blockchain can be used to augment such a solution, but it cannot provide the control to release such documents.

The IoT-based physical locks approach is similar to what we propose here. According to Sethuraman et al. (2022), Loki is an IoT-based key physical secure system. They propose an approach where physical objects are included in the security framework, allowing designers to consider physical secure systems alongside the software solutions. Likewise, several researchers that worked on smart lockers integrate embedded controllers and monitoring systems as well as diverse authentication methods in bank lockers, public storage, and home security. It is evident that the combination of these methods is along the lines of programmable, networked, and intelligent physical access controls. This study is along these lines, narrowing the focus on file protection and on-demand, energy-efficient biometric consensus.

Biometric fusion is another important area of research and development. Although unimodal biometric systems are quick and easy to use, they are typically ineffective. In a similar vein, multimodal and multi-instance biometric systems target the said challenge by integrating multiple biometric sources. This could be the combination of multiple biometric systems, such as, voice and face, ECG and fingerprint, or iris and fingerprint. In the current framework, fusion is also not in the plurality of body traits, but a plurality of fingerprint instances using several sensor pods. The idea is that a would-be attacker shouldn't be able to gain access by compromising one sensor. A configurable N of M policy allows secure systems to determine its operating requirements.

Research has shown potential benefits for combining multiple traits or channels for biometric systems. Gimba and others state that dual-channel or multimodal systems present greater reliability and resistance to counterfeiting than unimodal systems; however, those authors also state that the quality of design is a major factor for these systems. For the locker design, the presence of four sensors does not mean that the locker is securely designed. The quality of the integration of the sensors is crucial, along with controlled thresholds, template protection, anti-replay mechanisms, limits on access attempts, and tamper resistance. The presence of multiple sensors poorly integrated would yield an insecure locker system. However, an integration of multiple sensors would mean that the error of allowing access to the locker system due to a biometric capture would be highly mitigated.

Template protection is a critical factor in any biometric system design, due to the nature of the data used. Abdullahi and others provide an overview of biometric template attacks and countermeasures and indicate that attacks can be performed on biometric templates at multiple stages of the system. For a locker system, this indicates that the system of choice for a locker should not store raw fingerprint images in memory, and the template database should not be accessible to anyone with physical access. Thus, the proposed model provides local template protection and designs the system using the minutiae template system rather than the raw image system, supports the encryption of stored templates, and includes a means to purge the encryption key in the event of a tamper.

Standards help clarify generalized concerns and provide reference points for expected designs. ISO/IEC 19794 2 describes the standards for the representation and exchange of finger minutiae and defines fingerprint minutiae. NIST SP 800 76 2 details standards for biometric data associated with the personal identity verification process and defines preparation for interoperability of fingerprint, iris, and facial data as identity credentials. ISO/IEC 19795 1 provides guidance for the evaluation of biometric systems regarding error rates and throughput and the reporting of results. The current research uses these standards as anchors methodologically and does not assume certification. A standard allows the development of a design, while certification prohibits the development of a design. This distinction is important.

Concerns for energy efficiency also directly affect the design of IoT security devices. If a lock only functions when it has been recently charged, it is not a practical design for most offices, small data repositories, or rural institutional settings. The failure of many IoT security devices is not the failure of the security concept, but the failure to adequately align the security concept with the constraints of the operating environment, primarily the power budget. Core IoT device cybersecurity capabilities as described in NISTIR 8259A are of great use when organizations are establishing the means to manufacture, integrate, or procure IoT devices. An approach to consumer IoT security and

data protection is offered in ETSI EN 303 645. Although these publications do not provide guidance for battery design, IoT devices should be designed with a secure, sustainable, and life cycle considerations approach.

In file security, energy efficiency refers to something different than energy efficiency in continuous monitoring systems. The locker spends most of its time idling. During this time, it doesn't need all of its sensors, radios, and actuators fully active. The aim is to have the sensor authenticate, act, and record the event to low energy state. This event driven approach works nicely with duty cycling and sleep scheduling. Our design is based on the idea of wake in turn, and so does the rest. This is also a design to save energy. It can further reduce the number of interfaces active during idle time, which reduces the attack surface.

The existing literature focuses on different aspects, but there is a clear opportunity to contribute. There is significant research on biometric systems, smart lockers, IoT systems and security, and template protection. However, there is a lack of research on compact and energy efficient lockers for storing physical file bundles. In the existing research on digital lockers, the focus is usually on the management of cloud based documents. In the existing research on smart lockers, the focus is usually on home security or public storage. In the existing research on biometrics, the focus is usually on the evaluation of algorithms and systems for the protection of physical files. This research aims to create the technologies needed for this specific area, and is at the intersection of the above areas.

3. Research Gap and Contributions

This paper addresses the gap for a comprehensive, complete, power-aware model for multi-finger access control for protecting physical files. A mechanical file cabinet provides physical closure, but weakens identity assurance. A fingerprint lock provides identity assurance, but is still susceptible to a number of attacks, such as spoofing or sensor malfunctions. A threshold is also subject to attack. An IoT locker is an improvement, as it is capable of monitoring and logging, but may become impractical as it may rely too much on network availability or may require too much power. The model presented here attempts to bring the best aspects of each of these approaches together and to mitigate the majority of their weaknesses.

Another gap this model addresses is the way performance is reported. Many student and prototype smart lockers demonstrate a lock opens if a correct credential is presented and closes if an incorrect credential is presented. While this may be sufficient for a demonstration, it is not sufficient for a journal paper. Biometric systems must be evaluated on the basis of error measures, such as FAR, FRR, EER, and ROC analysis. For power, similar claims must be made at the component level and not in general terms, such as low power or energy saving. In this paper, the available readings are used to make such evaluations.

The study identifies five different areas of contribution. First is the development of the four sensor biometric file locker architecture that includes multiple points for capturing fingerprints and where the user can be in control of setting the authentication policy. The second contribution is the introduction of a power saving design for the authentication phase where a series of sensors in the architecture are designed to be active one at a time, while the rest remain in the sleeping mode. The third contribution combines a physical belt or latch design with tamper detection and lockdown mechanisms based on a worm gear or servo design. The fourth is the assessment of the performance of biometrics in terms of FAR, FRR, EER, and the evaluation of partial ROC using the set of thresholds. The fifth is a design for battery life showing how the combination of the state when the design is idle, during actuation, and the rate of unlocks in a day varies to allow for the long-term use of the design.

The more interesting factor is the design of a research apparatus that captures a valuable combination of existing technologies. The technologies integral to the design include fingerprinting, BLE, servos, and IoT logging. Many innovations in engineering occur at the point of integrating existing technologies, such as combining mechanisms for both security and convenience. A strong file security device must combine a high degree of security, low cost, simplicity, and high efficiency for continuous use. The proposed model is an attempt to satisfy all of these.

4. Materials and Methods

The study uses a design science and prototype evaluation approach. Design science is relevant since the goal is to create and examine an artifact instead of merely studying an existing system. In this case, the artifact is a model of a digital locker for physical files, which includes the hardware architecture, authentication flow, energy model and security control. Evaluation combines component level reasoning, biometric threshold, power, and scenario-based threat assessment. This combination of methods is suitable for an early stage of engineering study, in which the prototype is a sufficiently developed for supporting modeling and controlled testing, but is in more need of wide field testing before being deployed at large scale.

The research process was developed in phases. The first phase included writing the state of the art for fingerprint based locks, IoT security, digital lockers, and other biometric authentication and energy storage. In the second phase, the security challenge was translated into a proposed architecture based on a microcontroller in the line of the NodeMCU with a fingerprint reader, an OLED display, a servo or solenoid and other required electronic components. The third phase was the design locking of physical files with the use of a belt and multisensor and a sequence of authentication. In the fourth phase, design metrics were introduced, in particular FAR, FRR, TPR, FPR, EER and ROC. Finally, in the fifth phase, energy efficiency was introduced, with a model based on sensing that was not active all the time, but instead on a duty cycle.

The system under observation contains four fingerprint sensors, a controller with wireless capability, a display, control buttons, a locking actuator, a belt or latch structure, and optional audit communication. Earlier versions of the design contained NodeMCU. This component is often used to prototype IoT applications since it is economical and comes with Wi-fi. Promising energy optimized designs may utilize a low power system on chip with BLE, for example, the nRF52 class of controllers. This is an important distinction to make. For the early proof of concept, the NodeMCU is sufficient. However, as the system is to be deployed with a focus on the BLE and with the intention of long battery life, a different controller will be more appropriate. This is the reason the version of the journal contains the design of the architecture without the controller and explains both options.

The biometric approach is based on enrollment and subsequent verification. During enrollment, authorized users fingerprint is captured several times. The system can be designed to capture any four fingers or a certain predefined set of fingers, as per the organization’s policy. While verifying, the user has to present fingers to the sensors in the prescribed sequence or as per the system prompt. The controller performs the verification by comparing the captured templates to the authorized ones. Once the criteria of the required matches is satisfied, the lock is opened. In case the criteria is not satisfied, the access is denied, and the system records the event and enforces a lock to control the access attempts for a predefined time. This is a brute force attack deterrent.

The provided biometric data contain early sensor readings and an experimental threshold sweep model. Early sensor readings indicate that some calibration is required, as early sensor readings reflect high raw error rates due to unadjusted thresholds and capture procedures. The later threshold data are more appropriate for publication because they contain measurements for thresholds from 0.10 to 0.90, true accept, false accept, true reject, false reject, FAR, FRR, and TAR. Each of the sensors is tested in the threshold module for 100 genuine and 100 impostor trials. This data set is still controlled, and should be described as prototype and simulation based evaluation, instead of a population scale biometric evaluation.

FAR is defined as the ratio of false acceptances to the total number of impostor attempts. FRR is defined as the ratio of false rejectances to the total number of genuine attempts. TAR, expressed in percentage, is defined as 1 - FRR. The EER is defined as the operational point where FAR and FRR are equal. In a ROC analysis, the FAR is plotted against the TAR for various thresholds. As the provided threshold sweep covers only a portion of the operating region, a partial ROC and a normalized partial AUC are reported. It is incorrect to claim that a complete biometric AUC has been obtained, when in fact the data only allow for a partial AUC.

Power calculations on the component level are required by the energy method. For sequential authentication, one sensor draws 120 mW, while three stay in sleep mode, drawing 1.5 mW for a total authentication power of 124.5 mW. If the design is to have all four sensors permanently active, the total will be 480 mW. Therefore, the total power

savings for the active scanning interval is 355.5 mW or 74 %. Brief servo actuation, BLE advertising, and duty cycling of the sensors along with some other design elements are incorporated into the standby model. The battery used is a 12.2 Wh lithium ion cell based on an assumption to estimate long term running time.

The security assessment is based on scenarios. This model assesses the risk of unauthorized attempts to scan fingers, stealing or copying the template, attacking the system with a repeated number of attempts, cutting the system belt, moving the latch forcibly, replaying commands, and draining the battery. Each of these is linked to one or more of the following controls: multi-finger voting, local matching, encrypted templates, attempt control, tamper loop, worm gear, and voted command with deep sleep and offline first. This evaluation is not meant to replace a formal penetration test. It is a security analysis of the design to show what has been implemented and what needs to be verified by future tests.

5. System Architecture and Operational Design

The proposed architecture is a layered system. The belt, latch, worm gear or servo, sensor pods, and tamper loop comprise the physical layer. Fingerprint sensors, controllers, radios, displays, buttons, actuator drivers and circuits for power management comprise the electronic layer. The firmware layer covers enrolment, scheduling, matching, logging, and control of the lock and the communication functions. The security layer is concerned with protection of templates, counting and controlling attempts, command validation, and response to tamper actions. It is critical to design these layers in unison. A robust matching algorithm is of no use to secure a file if the belt can be cut without being detected. A tamper resistant belt is of no use if the controllers store templates in memory in an unprotected format. These components must function in harmony with good engineering.

The four sensor placement is a unique aspect of this model. The sensors can be positioned at the extremes or corners of the belt or locking surface; that is, the top left, top right, bottom left and bottom right. This use of geometry is advantageous in that it helps to distribute the points of authentication across the item being secured. It also helps to make the interaction more purposeful when compared to tapping a single sensor positioned at the handle. Depending on how the final enclosure is designed, the sensor pods can be either embedded in the belt housing or positioned around the lock body, or the pods can be distributed around the lid of a file. The industrial design of the system can vary, but the fundamental concept is that more than a single casual biometric action should be required to gain access to a secured item.

The controller is in charge of the authentication process. NodeMCU is ideal for the first prototype because it is flexible enough to interface with all of the required components and includes built-in network capability. In the future, Bluetooth Low Energy (BLE) with a system on chip would be ideal because it could significantly reduce energy consumption. The controller processes sensor input and wakes the required modules, requests a fingerprint, performs a comparison, and then updates the display to make the decision to unlock. The decision policy can be to deny unlock with any combination of sensors, or an N of M policy can be used if some flexibility with the sensors is required for usability.

The included display and buttons enable everyday usability. A small OLED display can be used to show warnings or prompts, or to indicate the status of the system (e.g. ready to scan user, access granted, access denied, etc.). Buttons can be used to support various functions (e.g. enrollment, scan, reset, and admin functions). These design elements help provide feedback that can minimize user rejection due to system misuse (e.g. placing a finger too early, etc.). An effectively designed system should be secure, yet allow consistent and clear operation to authorized users.

The locking system integrates control with resistive elements. For example, a servo motor with a worm screw or latch would allow locking without the need for continuous current. The worm screw is desirable, since the worm mechanism resists motion in the opposite direction, therefore making forced reverse locking more difficult. Although solenoids are simple and quick, they require more energy when in an energized state. As a result, the actuation for a battery powered file locker should be done in as short an interval as possible. The motor should move the latch and then, after confirmation, return the controller to the low energy state.

The belt design incorporates tamper detection. A continuous conductive loop placed in the belt or around the protected file pathway will result in a change of state to be recorded as a tamper event by the controller when the belt is cut, punctured, or disconnected. A more advanced design will permanently erase all cryptographic keys and stored biometric templates from the system, preventing subsequent usage by an attacker, in response to a tamper event. The system should be designed in such a way that it will not trigger a tamper event for an accidental break or loss of the power source. However, without establishing tamper detection, a physical attack to breach the storage system would be more effective than attacking the system's point of authentication, which in this case is the biometric locker.

The workflow locks and stands by when not in use. The system is at a low power state. That system switches states when the user starts an authentication. In this phase, the first sensor activates while the other sensors remain asleep. Once done and verified, the controller activates the subsequent sensor. This process continues until the decided matching condition is achieved. Once the actuator unblocks the mechanism and the display shows the success message, the process is completed. If one or more of the sensors does not match, the system logs the attempt, goes back to the locked state after a time delay, and fails the authentication. While this process seems a bit longer than a normal authentication process, the extra time is a small price to pay for the enhanced security of a system that controls access to sensitive information.

To maintain privacy and security, matching of the fingerprints is done on the system and the only feedback to the controlling system is an accept, reject, low battery, or tamper indication. It is an unnecessary privacy and a security risk to provide raw biometric data for a network. Control of the stored templates must be secure and administration must be done on the system itself. The controlling system, when available, must use secure communication to maintain the operational integrity of the locking mechanism.

The next figure shows the system architecture and how the sensors, tamper loop, controller, template store, actuator, display and audit channel are related.

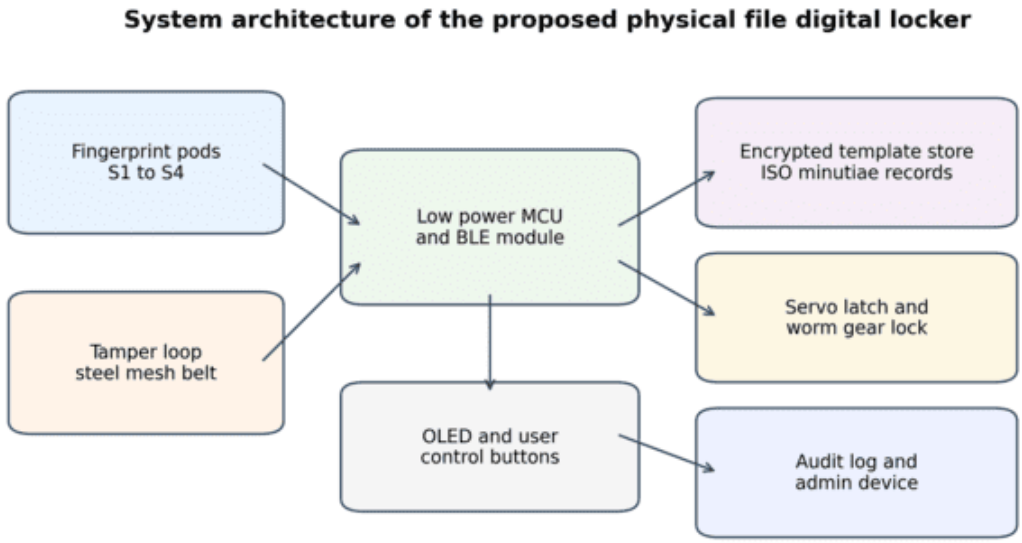

Figure 1. System architecture of the proposed biometric digital locker for physical files.

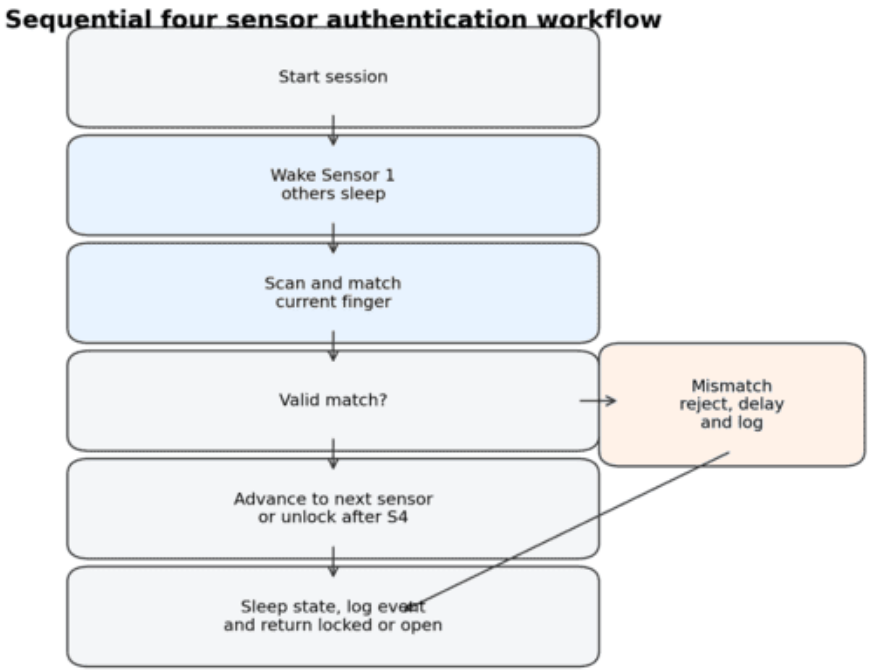

Figure 2. Sequential four sensor authentication workflow with rejection and sleep return path.

6. Energy Model and Security Model

The feasibility of the locker proposal relies heavily on energy efficiency. If a highly secure design requires lots of energy (frequent charging), it will likely be left uncharged. To avoid spending so much energy on charging, we expect the system will spend most of the time idle and will only be frequently active for short bursts during the authentication process. Because of the expected operating condition, the power budget becomes sensitive to a number of design choices. The proposed design is built on the logic of event-driven operation: it is quiet the device when idle, it wakes the minimum required components to authenticate, and it completes the authentication actions and returns to sleep.

The most prominent energy saving design feature is the the use of a sequential sensing strategy. In the provided simulation, one active sensor consumes 120 mW while each sleeping sensor consumes 1.5 mW. During authentication, the sequential model thus consumes 120 mW + 4.5 mW for the sleeping sensors, or 124.5 mW. Systems employing a four sensor architecture with constant activity consume 480 mW. The savings during the scan window is thus 355.5 mW, or approximately 74 percent. Daily consumption for the system will not be less 74 percent due to idle radio consumption and the energy used to drive the actuators, but it will be much more energy efficient.

The standby model requires BLE advertising and sensor duty cycling. The provided energy data estimate 50 microamps at 3.3 V for low duty cycle BLE advertising, resulting in ~3.96 mWh consumed daily. Fingerprint sensors on are duty cycled in a round robin manner resulting in an average current of 37.5 microamps at 3.3 V, consuming ~2.98 mWh daily. Together, these idle loads result in an average of ~6.9 mWh daily. The servo actuator consumes ~0.25 mWh of energy for each unlock. If we assume up to 20 daily unlocks, actuation would consume 5 mWh daily. From this, we can estimate total daily energy consumption to be ~11.9 mWh. With a 12.2 Wh lithium ion cell this would result in an estimated battery life of 2.8 years (or 1025 days).

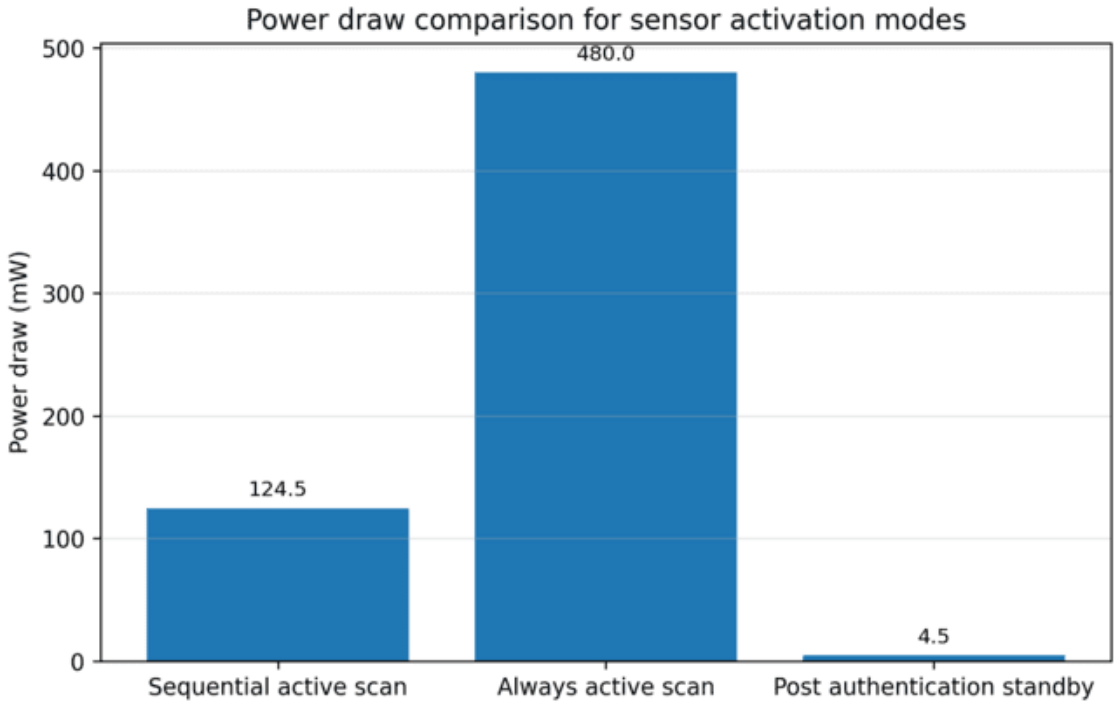

Figure 3. Power draw comparison between sequential active scanning, always active scanning and post authentication standby.

These estimates are of course rough. Actual battery life will depend on a number of factors including temperature, aging, load, friction, failed unlock attempts, self discharge, bugs, and radio settings. A file locker in an air conditioned office may perform differently from one in a dusty archive. The value of this model is that we make the assumptions explicit. In the future, improved iterations of this prototype can replace the assumed current values with actual current measurements obtained via an oscilloscope or a power analyzer.

The security model applies a layered approach. The biometric layer introduces barriers to key sharing and PIN disclosure. The multi finger layer reduces reliance on a single sensor or a single biometrics instance. The layer of template protection reduces the threat of leaking biometric information. The mechanical layer stops easy or trivial openings. The tamper layer identifies the attack on the belt. The logging layer establishes responsibility. The energy layer introduces protection against the threat of battery depletion. None of the measures is fully effective. However, combine them, and they offer a more robust defense against a simple fingerprint swiping attack.

One of the primary design decisions is the severity of the N of M policy. When the requirement is four of four, the assurance level is higher, but the usability level is lower, due to possibly rejecting legitimate users when one of the fingers is injured, dirty, or inappropriately positioned. If the requirement is three of four, the usability level is improved, while the assurance level is still higher than in a one sensor policy. Two of four is an adequate requirement for a low threat environment, but is inappropriate for a high threat environment. This paper does not impose a monocentric approach. Rather, it suggests thelocker should offer the setting, and the associated organizations should decide based on sensitivity of the documents, size of user groups, and their operational tolerance of being locked out.

One more straightforward, but useful control is attempt throttling. The system should not allow infinite retries after an attempt is rejected; instead, the system can implement a small delay after a failure, with the delay becoming longer with each failure. Administrative intervention after a certain number of failures can also address the issue of casual system abuse and brute force attacks. The delay should not be so long as to punish a legitimate user for an unsuccessful scan. This control perfectly demonstrates the balance of security and system usability. Users will

circumvent the system if they find the controls to be overly strict, and a relaxed system fails to adequately protect itself.

The design being proposed considers network connectivity to be optional, not mandatory. The system can log data and perform administrative functions via secure BLE. Additionally, the system can be designed in such a way that unlocking does not require cloud connectivity unless the particular deployment has chosen to require remote approval. This is a preferred design for a system being used in an environment where there are poor and unreliable network connections, frequent network outages, and firewalls that are overly restrictive. A file locker system should never fail to operate (open/locked) based on network connectivity. It should, however, fail to operate (close) when there are local users.

7. Results and Analysis

Data was analyzed with respect to three key questions. First, what is the behavior of the biometric component across thresholds? Second, what is the impact of the activation of the remaining sensors? Third, what can the daily energy budget tell us about actual deployment? The analysis is conducted based on the provided prototype and simulation data. It does not suggest that the prototype has passed the first population scale biometric certification. It aims to present the available measurements in a clear journal paper style. It aims to illustrate how the design can be assessed in a more structured way in future work.

A sweep of the biometric threshold shows the typical tradeoff of FAR and FRR. At low decision thresholds, the system is rather permissive. In this case, genuine users, or non-malicious users, are almost always accepted, so the FRR remains low, however in an implicit way, the system provides a higher acceptance rate to attacks, thus increasing FAR. In contrast, at high decision thresholds, the system becomes rather restrictive. In this case, a higher match score is required, therefore more genuine users are rejected. This behavior is typical for any biometric system, and to support the usability of the system, it is evident that in determining which threshold to choose, a balance needs to be struck between security and system usability.

In a typical threshold table, the practical crossover lies at about 0.50. The average false acceptance rate (FAR) at this threshold is around 3.67 percent, and the average false rejection rate (FRR) is around 4.21 percent. The resulting equal error rate (EER) is estimated at approximately 3.94 percent. While this is not an ideal operating point, it is an acceptable result for early stage prototyping and modeling. From this, it can be reasonably concluded that the model does a fair job of distinguishing between genuine attempts and impostor attempts for this given range and that the error rates may be improved by the quality of the model and the quality of the images used, and the quality and detection of liveness in the subjects during enrollment.

The per sensor results show some variation for the four positions. In the supplied data, Sensor 2 has the best result at an estimated EER of 3.24 percent. This is followed by Sensor 1 with an EER of 3.70 percent. An EER of 4.05 percent is recorded for Sensor 4 and Sensor 3 has an EER of 4.74 percent. This variation is helpful as it directs the designer to the appropriate location for hardware refinement. A lower performing sensor may be influenced by improper positioning, cable noise, low quality sensor modules, or improper capture angles. In a final prototype, each pod should be calibrated independently, as identical performance should not be assumed.

Table 1. Per sensor biometric performance summary from the supplied threshold sweep.

Sensor	Location	EER threshold	FAR at EER (%)	FRR at EER (%)	Estimated EER (%)
Sensor 1	Top-left	0.50	3.45	3.96	3.70
Sensor 2	Top-right	0.50	3.02	3.46	3.24
Sensor 3	Bottom-left	0.50	4.42	5.07	4.74
Sensor 4	Bottom-right	0.50	3.77	4.33	4.05

The partial ROC plot reinforces threshold behavior. All four sensors work in the high TAR region. TAR ranges differ in the measured operating range. Due to the lack of coverage in the data for the complete range of TAR, this paper presents a partial ROC and does not claim a full AUC for certification. When the partial area is normalized in the observed TAR range, the sensors are in the range of 0.962 to 0.975. This indicates a high degree of discrimination in the tested range and should not be directly compared to full range AUC values of large public biometric data set.

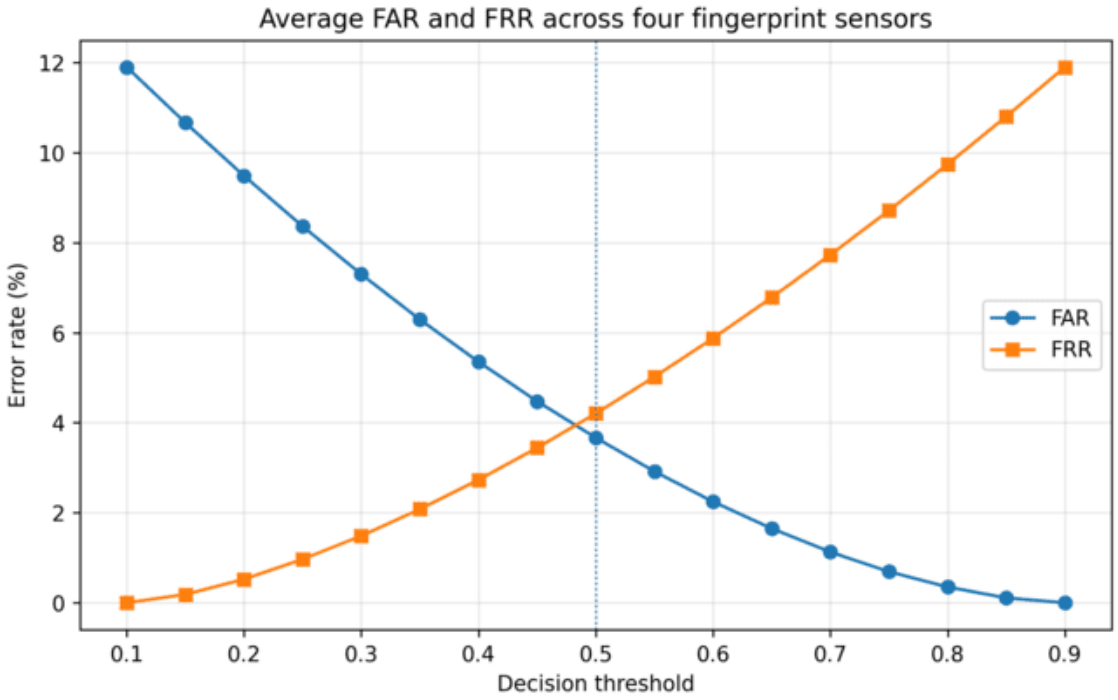

Figure 4. Average FAR and FRR tradeoff across decision thresholds.

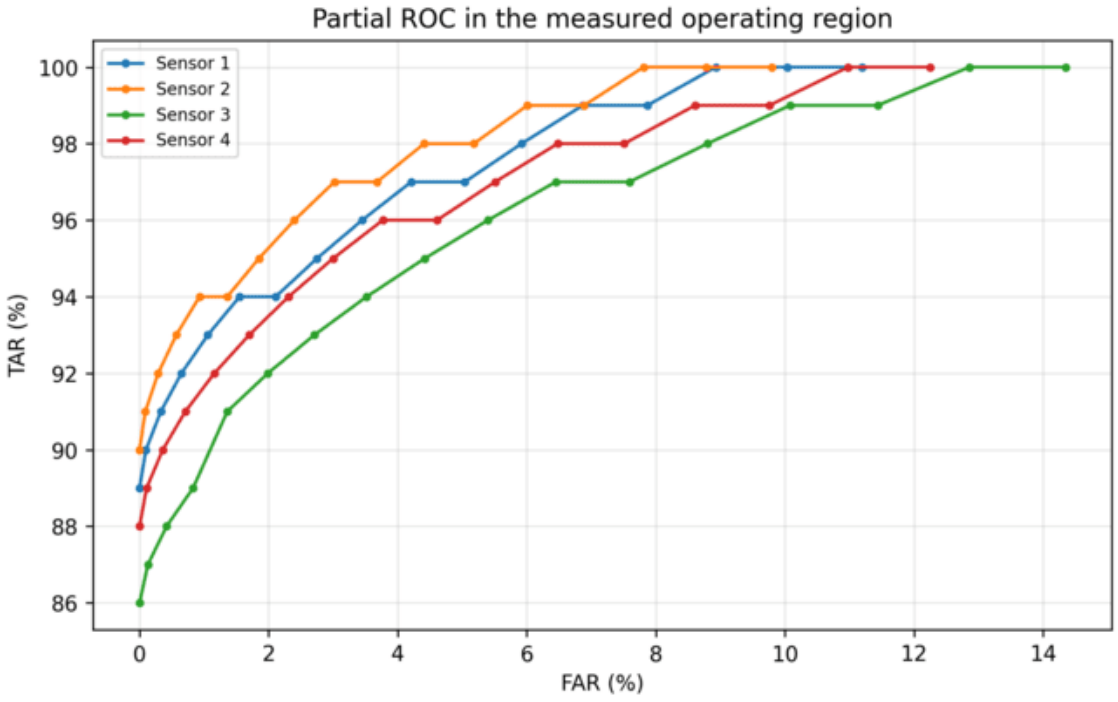

Figure 5. Partial ROC view for the four sensors in the measured operating region.

The comparison of the power is more direct. During the active authentication process, the power consumption of the sequential scanning was 124.5 mW compared to 480 mW, which is the power consumption of the four sensor model in the fully active (always on) state. The large difference confirms the design idea that while a sensor is not in use, it can be powered down. The post authentication state is a stand by (low power) mode and its power consumption is 4.5 mW, which is a significant (large) difference compared to the fully active state. The actual value of the stand by mode will be determined by the selected microcontroller and the setting of the radio, but the important thing is the relative lesson: duty cycle is very important for a long battery.

The battery model demonstrates how everyday use alters everyday run time. With five daily unlocks, the battery is estimated to last almost four years. With twenty daily unlocks, battery life drops to an estimated 2.8 years. With eighty daily unlocks, battery life is estimated to drop to less than one and a half years. This is a typical scenario, considering that every daily unlock requires a form of actuation. Despite this model having limits, it is still reasonable to assume it could be deployed in an office environment, as long as the battery is either rechargeable or replaceable. The more likely concern would be an uncontrolled drain in idle use, as the power is consumed every hour, regardless of daily unlocks.

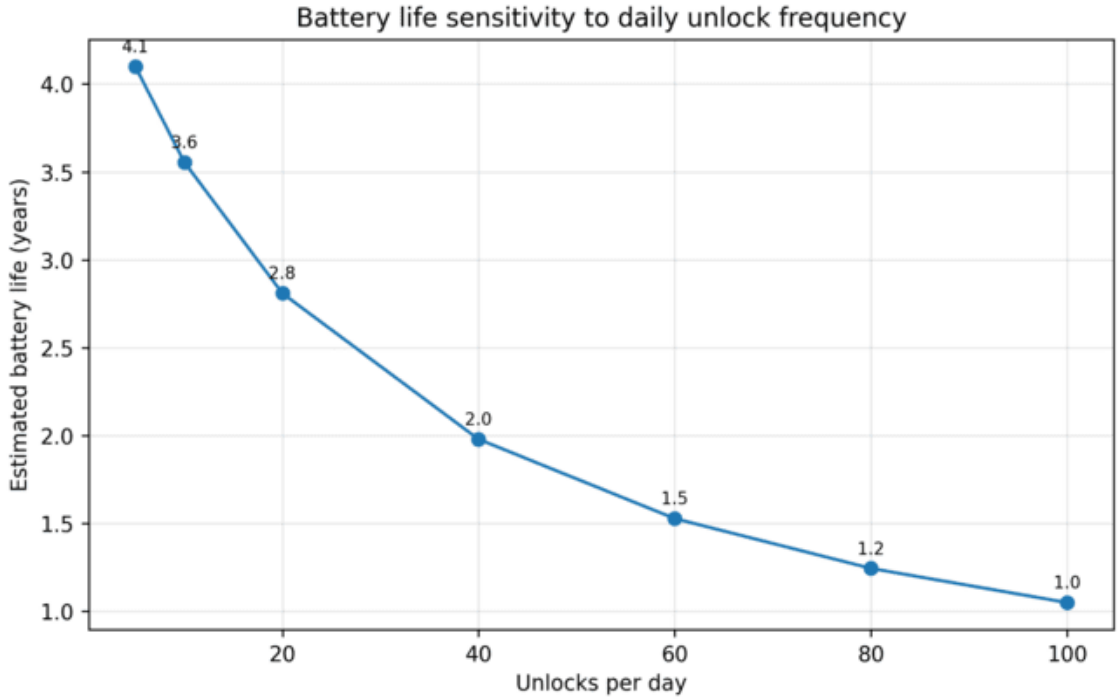

Figure 6. Estimated battery life sensitivity under different daily unlock frequencies.

The early experimental notes in the provided reports also document rough FAR and FRR values from first time testing. These figures should be seen as preliminary calibration data rather than final performance data. These figures advocate the necessity of a full threshold tuning as well as a refined evaluation. It is very tempting to withhold poor primitive results, but in this case, poor results justified a shift to conduct a threshold sweep, as well as selecting operating points more clearly.

The threat control analysis indicates that this system is most likely the strongest against casual unauthorized access, key sharing, PIN sharing, and simple forced opening. It is also better than a single sensor design against isolated capture errors or one sensor spoofing. It is not as strong, however, against advanced presentation attacks, unless liveness detection is implemented. It requires formal evaluation for advanced defenses against physical tampering,

side channel attacks, template attacks, and battery drain attacks. This is important to differentiate. The current design is encouraging, but a product that is deployed would need a hardware security review a firmware audit, and environmental testing.

The assessment results indicate that the system design is encouraging. The biometric model establishes a measurable operating point. The energy model indicates the potential for long run time. The security model establishes meaningful controls. Therefore, the system is more than a conceptual locking system. It is a structured cyber-physical access control system model for physical files that is ready for more detailed prototype testing and refinement.

8. Discussion

This study indicates that physical file security can be advanced by the use of biometric consensus in conjunction with energy aware embedded design. The largest gain is not that the locker is impossible to bypass. The truth is that there is no device that can honestly claim that. The true gain is that the cost of unauthorized access is greater, while the accessibility for the authorized user is kept at a reasonable level. A user can no longer obtain the file by borrowing the key or guessing the PIN. Now, a user must satisfy the biometric requirement and defeat a physical lock that audits access. For many offices and archival repositories, that is a significant step forward.

The design of the multiple fingerprint requirement creates a different psychology around access. A single fingerprint lock can be viewed as a convenience feature. A requirement to access a file by means of a four sensor sequence can be viewed as a secure ritual. In a given context, the design of the file security system can make a great deal of difference. When the system is designed to make the eventual access of a file a high degree personal event, recorded, and more difficult to share, casual file misuse is less likely. In the design, the misuse of the system should not be a rout. Therefore, the design must be user tested, particularly in relation to the sequence of scans, the prompts, the positioning of the hand, and the recovery from a failed attempt.

These results also illustrate how threshold selection and biometric performance are intrinsically linked. A sensor does not have a single, immutable, accuracy value. As the decision threshold shifts, so do the errors. For highly sensitive information, the administrators may choose to have a lower FAR at the cost of increased FRR. For less sensitive information, they may choose a higher FAR, and lower FRR. The flexibility to choose to set specific policies is an ability of the system, but the policy should be made known. A system should not defend its accuracy and say that it is accurate. It should specify the threshold, the distribution of the trials, and the tradeoff with error.

Context matters to energy efficiency, and a 74 percent reduction is significant, but the user cares more about how often they need to replace the battery. That explains the system's energy model and the drain during advertising is the tradeoff that is most relevant. The balance of the hardware and the firmware can be the difference between an unacceptable product and one that is acceptable. A controller can poll sensors and advertise. The most important suggestion from the energy analysis is to take current measurements on the targeted hardware and not rely on the datasheets.

In context of existing smart locker literature, there is a discernible design trade-off. A number of more contemporary smart locker systems offer a wider set of authentication methods, such as One Time Passwords (OTP), facial recognition, RFID, emergency codes, and mobile app interfaces. While this greater system flexibility is a positive system design attribute, it also results in higher system complexity. The present iteration of the file locker is more constrained. It focuses on local biometric consensus, physical tamper resistance, and low power consumption. For some deployments, this may be preferable to a more resource cloud intensive system. A small law office or record storage room in a school may prefer a system that operates reliably without the burden of a complex user database and online connectivity.

Another consideration that favors the design is local processing. Fingerprint template data can be sensitive and a system that transmits raw biometric data to the cloud can create a trust burden that may be difficult for many organizations to manage. The design proposes keeping the matching process on the device and storing templates in encrypted form. While this does not eliminate the privacy risk it does provide a measure to limit the exposure. Future

iterations should address this risk with stronger privacy protections and improve the design with the use of secure elements and formal key management. The risk is serious if a storage device with templates is compromised, as biometric data cannot be revoked or changed.

The design has social and organizational effects as well. A staff file locker is likely to be used by several employees. Policies should govern the enrollment and removal of staff, as well as granting emergency access and conducting audit reviews. A device can be implemented by a technique with a high level of security, but the organization can defeat the purpose by poor handling of enrollment. Biometric systems become a design feature and a barrier that is easy to circumvent if an administrator enrolls a shared fingerprint, keeps a backup of credentials in an insecure place, or does not remove staff who have left the organization. Therefore, the deployment of the systems should be accompanied by administrative procedures, user training, and audits that are conducted regularly.

Another important factor is dealing with failures. What should occur if a sensor fails, the battery runs out, a user is unable to provide access due to an injury, or the tampering protection device is broken? A system that is secure needs several options to address these kinds of failures, but having the options creates a risk that the system is not secure. Emergency access should be designed in such a way that dual administrative approval is required, and a permanent audit record is created. Addressing a failure should not be accomplished by a hidden switch that renders the security design ineffective.

Despite the constraints, this study is important because it presents the security of physical files as a quantifiable subsystem of cyber-physical systems. There are still many organizations that consider file security as something involving keys and cabinets. This paper argues that the design of physical file security systems can incorporate modern, embedded systems while still considering cost, battery, and daily convenience. The design is not a final, market-ready system, but a reasonable research platform for future work.

9. Limitations and Future Work

There are a number of factors that limit this study. Firstly, with regards to the biometric evaluation, the provided threshold sweep is valuable to estimate FAR, FRR, and EER; however, this is not a complete biometric evaluation. Future studies should involve greater participation and include more sessions, varying conditions of the participants (e.g. varying moisture levels in fingers, minor injuries, contact with dust, etc.), more natural user errors, and more artifacts. It should differentiate the false match rate at the algorithmic level and the false acceptance rate at the system level, as both require multiple attempts and user interaction to define.

The other limitation is that this study does not include any liveness detection testing. There are a number of ways to violate the integrity of a fingerprint system by using replica fingerprints, high quality casts, or lifted impressions. Although multi-finger policies increase the difficulty of the attacks, they do not eliminate the need for presentation attack detection. Future studies should examine liveness detection created by varying levels of pressure, a pulse, or conductivity. It should also include a challenge-response finger prompt and other sensor modules that contain certified anti-spoofing elements. Until then, this study cannot state that it is resistant to advanced spoofing.

The third limitation is mechanical validation. Although the worm gear and belt concept would resist casual opening, actual security relies on the tamper loop’s durability, latch design, enclosure design, and material strength. The effects of cutting, prying, and twisting, as well as the effects of extreme temperatures, sustained use, and the addition of mass and intentional tampering should also be analyzed. The lock should be tested for wear after being cycled to the open and closed positions thousands of times. Biometric security mechanisms are often thought to be more secure than their mechanical counterparts. However, mechanical failure or security design errors can result in the same situation, which is loss of control over access to physical resources.

The fourth limitation is energy measurement. The current model is based on speculation and supplied components. A final study should measure current in the provided states for the sleep, standby, scan, match, and communicate and actuation states. Additionally, it should evaluate the effects of extreme temperatures and aging on the battery. Heuristic evaluations of power consumption in IoT systems often look promising, but actual consumption

can change when other components such as firmware libraries are included. This is not a shortcoming of the current study, but a typical shortcoming of the field of embedded systems.

The fifth limitation is control. While this study attempts to provide a technical framework, control mechanisms and policies are required for deployment. Future studies should provide details on the biometric data collection process, emergency data access policies, data auditing, and retention policies. While control mechanisms may reduce the privacy risks of unregulated biometric data collection, they should not create privacy harms in the process.

There are four avenues for future development. The first is the creation of an improved hardware prototype that incorporates a low power BLE controller, a secure element, calibrated fingerprint pods, and a tested latch enclosure. The second is the creation of a user study consisting of multiple test sessions and 50-100 study participants. The third is a security study that investigates the risks associated with template extraction and replay, as well as spoofing and tamper attacks. The fourth is the implementation of an institutional pilot in a controlled records room that would log the access, battery life, and the overall ease of use for the system over many months. Each of these development avenues would establish a significant milestone in the evolution of the system that would take it from the design study of a deployable research system to a fully deployable research system.

10. Conclusion

This paper introduced a model for a digital locker that employs a multi finger biometric system and additional features for energy efficiency. The model aims to solve a real-world problem: sensitive paper-based records are still in use, and the existing file locker solutions in the market do not offer the necessary assurance for one's identity, auditability, and awareness of the tamper state. The architecture design proposes the integration of four fingerprint sensors with local template protection, Internet of Things (IoT) based control, a display, servo actuators, a tamper sensor, and energy management through duty cycling.

The preliminary data provided shows that the proposed design is feasible. Under the proposed design, the operating point for biometrics is a threshold 0.50 under which an Equal Error Rate (EER) of 3.94 is estimated with sensor specific variation and calibration. When the sensors are activated in sequence, the power consumption for the authentication system drops from an overly active 480 mW to 124.5 mW; an approximate 74% savings during the scanning operation. Under the proposed design, the daily energy model estimates a 2.8 year operating life under a 12.2 Wh cell with 20 daily unlocks. This proves that an enhancement to the control of physical file access can be achieved without the use of constant power demanding sensors.

This study should be understood as a detailed evaluation of prototype and design in lieu of commercial certification. Further research will include studies on larger biometrics, liveness testing, and incremental assessment of power and peripheral stress testing. The model on the other hand, shows how integration of biometric consensus, control of IoT devices, and low energy, adaptive firmware can be combined into a practical security system to safeguard physical documents. Within organizations where physical paper documents exist in a legally or administratively valuable form, this system is a substantial advancement in security technology compared to traditional locks, and keys, or systems requiring the input of a PIN.

11. Consolidated Tables for Journal Submission

Table 2. Main design elements and their roles in the proposed system.

Design element	Implementation in the proposed model	Purpose
Four fingerprint sensors	Sensor pods placed around the physical file belt or lock surface	Improves assurance by requiring multiple biometric presentations
Sequential wake scheduling	Only one sensor remains active while others sleep	Reduces scan phase power draw and unnecessary active interfaces

Encrypted template storage	Minutiae based templates stored locally and protected by device keys	Reduces exposure of raw biometric information
Servo or worm gear latch	Short actuation pulse with reverse motion resistance	Provides physical locking without continuous hold current
Tamper loop	Conductive loop through belt or lock body	Detects cutting or forced attack and supports audit or key purge
Local audit log	Accepted, rejected, failed and tamper events stored locally	Creates accountability even when network is unavailable

Table 3. Selected average threshold readings across the four sensors.

Threshold	TA	FA	TR	FR	FAR (%)	FRR (%)	TAR (%)
0.10	100	12	88	0	11.90	0.00	100.00
0.25	99	8	92	1	8.36	0.97	99.00
0.40	97	5	95	3	5.35	2.73	97.25
0.50	96	4	96	4	3.67	4.21	96.00
0.60	94	2	98	6	2.25	5.88	94.00
0.75	91	1	99	9	0.69	8.71	91.25
0.90	88	0	100	12	0.00	11.90	88.25

Table 4. Energy model used for battery life estimation.

Component	Power or current assumption	Daily energy estimate	Interpretation
BLE advertising	Approximately 50 microampere at 3.3 V	3.96 mWh per day	Maintains low duty wireless availability
Fingerprint sensors	Average 37.5 microampere at 3.3 V	2.98 mWh per day	Represents round robin sensor duty cycling
Idle total	BLE plus sensor standby	6.9 mWh per day	Baseline consumption before unlock events
Servo actuator	0.3 A at 6 V for 0.5 second	0.25 mWh per unlock	Short pulse avoids continuous holding current
Daily total at 20 unlocks	Idle plus twenty actuator events	11.9 mWh per day	Supports about 2.8 years from a 12.2 Wh cell

Table 5. Threat control matrix for the proposed physical file locker.

Threat scenario	Control in proposed design	Residual issue requiring future testing
Unauthorised user presents one finger	Configurable N of M multi finger policy	Full impostor trials are needed with larger populations
Repeated guessing or rapid attempts	Attempt throttling and event logging	Delay policy must balance security and usability
Template extraction from memory	Encrypted local templates and key purge on tamper	Secure element and firmware audit recommended

Physical cutting of belt	Conductive tamper loop and steel mesh structure	Mechanical force testing is required
Forced latch movement	Worm gear or servo latch with reverse resistance	Enclosure attack tests are required
Battery drain attack	Duty cycling, low power standby and battery monitoring	Real current trace validation is required
Network outage	Offline first local matching and local audit storage	Synchronisation policy needed after reconnect

12. Practical Deployment Protocol and Reproducibility Considerations

When submitting research on an embedded security prototype, the journal expects more than just a working circuit. The researcher must establish boundaries on the prototype so it is possible for the reviewer to replicate the device and the researcher's measurements and determine if the claims are sustained outside the laboratory. For this reason, the proposed locker is intended to be deployed in three phases. The first phase is validation on a bench. The controlled first phase incorporates the testing of the NodeMCU, fingerprint sensors, display, actuation mechanism, belt assembly, and power supply both individually and in their final integrated assembly. At this phase, it is not the goal to test ultimate security. It is the goal to test and confirm predictable behavior of each subsystem. Measurements for sensor wake time, template matching time, servo actuation time, sleep current, and recovery after a failed scan, are to be taken during each test. It is important to note that the faults in many IoT prototype tests are not due to the biometric algorithm, but rather due to poor and unstable wiring, poor grounding, voltage fluctuations, and inconsistent loading in the mechanical components.

The second stage is repeated user-level authentication testing. A usable system would differentiate logs for valid, invalid, and erroneous attempts. Valid attempts would include known users placing fingers under varying conditions such as different finger placement, rotation, pressure, or moisture. Impersonation attempts would include unknown users attempting to unlock the belt without knowledge of the unlocking sequence. Operational error attempts would include placing fingers incorrectly, drawing fingers too quickly, too many attempts, or an incorrect sequence. Separately reporting these attempts helps ensure the evaluation does not conceal system usability issues behind a single, combined error rate. It also adheres to the biometrics standard, which requires the population/sample, transaction type, decision rule, and failure to acquire conditions not to be considered background information (ISO/IEC 19795-1, 2021). This means that all authentication transactions should capture the attempt type, position, threshold, decision, response time, and state.

The third stage involves testing the document security system in the real world. Unlike the virtual world, where the user interacts with a login system through the screen, a file locker is real world tangible object, which means, an attacker can directly interact with the locker. The attacker can pull the belt, press the clasp, or tamper with the sensor, or even try to make the actuator operate in a failure condition. Thus, testing in the real world is required to check the response to mechanical tampering and stress. The belt and clasp should also be tested for loosening and misalignment. Additionally, the clasp should be checked for failure to relock after successful opening and also after accidental unlocking due to vibrations. The belt should be checked for failure to relock after tampering and testing. Removing the cover, shorting, and tampering with the controller should be done to evaluate the detection of tampering. The paper should not mention the resistance to advanced hardware attacks without the invasive security testing. It is best to say that the design incorporates a higher security level and a more tamper evident design, in addition to several less accessible attacks, such as sensor spoofing, side channel attacks, and microcontroller attacks which require a lab setting.

In the interest of reproducibility, the final manuscript must include a minimum bill of materials, code, selection of thresholds, and the corresponding calculations of energy. Although the present study offers the information necessary to study the basic energy difference of the sequential model and the four-sensor always-on baseline, still, reviewers may want to know if the energy saving observed is due to the authentication policy, or does it rather come

from the selected hardware. The answer includes both. The savings are attributed to the sequential policy as the scanning made the decision to activate one sensor and the rest remain in sleep. However, the savings are determined by the active current and sleep current of the selected sensors, the time the scan takes, the sleep mode of the microcontroller, and the number of unlock attempts in a day. For this reason, the study states the assumptions and incorporates a sensitivity analysis rather than presenting the estimate of battery life as a fixed value. This kind of transparency is intended to make defending the work during peer review less difficult, and subsequent iterations of the work easier to augment.

Lastly, the submission should be framed as a prototype-based design and evaluation study, as opposed to a turnkey commercial security certification. The most remarkable aspect is the synthesis of integration of physical document security, multiple finger biometric, and the sequential low power operation along with the measurement of FAR, FRR, EER, ROC, and energy results. The current limitation is the lack of public benchmarks because the data is collected from a prototype and threshold sweep instead of a large external biometric dataset. This is not a reason to reject the work, but should be stated. Credibility of the work is to a large degree based on what it can demonstrate now, and what it must be validated on later. It can be claimed on these grounds that the system marks a significant and worthwhile improvement in the state of low power biometric security for documents in offices, university departments, storage research archives, and small institutional record storage rooms.

13. Declarations

Conflict of interest: The author has no conflict of interest regarding this draft.

Funding: The author reports no external funding for the preparation of this draft. Any funding from an institution or a project must be reported prior to the publication of this draft.

Data availability: The data presented in this manuscript are from the prototype progress report, the simulation module, and biometric thresholds. Complete and unedited trial logs must be presented or deposited prior to the publication of this draft.

Ethical consideration: This draft uses data from a prototype and simulation. Any biometric user study conducted afterward must have informed consent and must define the rules for data retention and must safeguard the biometric templates per the policy of the institution, applicable law, and the standards of the biometric industry.

REFERENCES

1. Abdullahi, S. M., Sun, S., Wang, B., Wei, N., & Wang, H. (2024). Biometric template attacks and recent protection mechanisms: A survey. Information Fusion, 101, 102144. https://doi.org/10.1016/j.inffus.2023.102144
2. Alzhrani, A. A., Balfaqih, M., Alsenani, F., Alharthi, M., Alshehri, A., & Balfagih, Z. (2024). Design and implementation of an IoT integrated smart locker system utilizing facial recognition technology. Engineering, Technology & Applied Science Research, 14(4), 16000 to 16010. https://doi.org/10.48084/etasr.7737
3. Arias Cabarcos, P., Almenares, F., Marín, A., Díaz Sánchez, D., & Sánchez Guerrero, R. (2019). A systematic literature review of adaptive authentication systems. ACM Computing Surveys, 52(4), 1 to 30.
4. ETSI. (2024). ETSI EN 303 645 V3.1.3, Cyber security for consumer Internet of Things: Baseline requirements. European Telecommunications Standards Institute.
5. Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). IoT device cybersecurity capability core baseline (NISTIR 8259A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259A
6. Gimba, U. A., et al. (2025). Enhancing biometric authentication through multimodal approach combining face and fingerprint recognition using convolutional neural networks. Discover Computing.
7. Grother, P., Salamon, W., & Chandramouli, R. (2013). Biometric specifications for personal identity verification (NIST SP 800 76 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-76-2
8. International Organization for Standardization and International Electrotechnical Commission. (2011). ISO/IEC 19794 2:2011, Information technology, Biometric data interchange formats, Part 2: Finger minutiae data.
9. International Organization for Standardization and International Electrotechnical Commission. (2021). ISO/IEC 19795 1:2021, Information technology, Biometric performance testing and reporting, Part 1: Principles and framework.
10. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4 to 20. https://doi.org/10.1109/TCSVT.2003.818349

11. Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. EURASIP Journal on Advances in Signal Processing, 2008, 579416. https://doi.org/10.1155/2008/579416
12. Nappi, M., Riccio, D., & Ricciardi, S. (2018). Context awareness in biometric systems and methods: State of the art and future scenarios. Image and Vision Computing, 76, 27 to 37.
13. National Institute of Standards and Technology. (2025). Digital identity guidelines: Authentication and authenticator management (NIST SP 800 63B 4). https://doi.org/10.6028/NIST.SP.800-63b-4
14. Sethuraman, S. C., Mitra, A., Li, K. C., Ghosh, A., Gopinath, M., & Sukhija, N. (2022). Loki: A physical security key compatible IoT based lock for protecting physical assets. IEEE Access, 10, 112721 to 112730. https://doi.org/10.1109/ACCESS.2022.3216665
15. Singhal, J., Gautam, A. S., Bhatia, A., Agrawal, A., & Kaushik, R. (2022). DD Locker: Blockchain based decentralized personal document locker. International Conference on Information Networking, 68 to 73. https://doi.org/10.1109/ICOIN53446.2022.9687236
16. Temoshok, D., Fenton, J., Choong, Y. Y., Lefkovitz, N., Regenscheid, A., Galluzzo, R., & Richer, J. (2025). Digital identity guidelines: Authentication and authenticator management (NIST SP 800 63B 4). National Institute of Standards and Technology.
17. Velasquez, I., Caro, A., & Rodriguez, A. (2018). Authentication schemes and methods: A systematic literature review. Information and Software Technology, 94, 30 to 37.
18. Yang, W., Wang, S., Shahzad, M., & Zhou, W. (2021). A cancelable biometric authentication system based on feature adaptive random projection. Journal of Information Security and Applications, 58, 102704.
19. Zhang, X., Wang, Z., Li, Y., et al. (2020). DeepKey: A multimodal biometric authentication system based on EEG and gait. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies.
20. Zulfiqar, M. I., & Younis, I. (2024). Enhanced security paradigms: Converging IoT and biometrics for advanced locker protection. IEEE Internet of Things Journal, 11(20), 33811 to 33819. https://doi.org/10.1109/JIOT.2024.3432282
21. Appendix A. Full Average Threshold Sweep
22. Appendix Table A1. Full average readings used to estimate the operating threshold.
23. Appendix B. Energy Equations
24. Sequential scan power = one active sensor power + three sleeping sensor powers = 120 mW + 3 x 1.5 mW = 124.5 mW.
25. Always active scan power = four active sensors x 120 mW = 480 mW.
26. Scan phase saving = 480 mW minus 124.5 mW = 355.5 mW, equal to approximately 74 percent.
27. Idle energy per day = BLE advertising energy plus fingerprint sensor duty cycle energy = 3.96 mWh + 2.98 mWh = approximately 6.9 mWh.
28. Daily energy at twenty unlocks = 6.9 mWh + 20 x 0.25 mWh = 11.9 mWh.
29. Battery life = battery capacity divided by daily energy = 12200 mWh / 11.9 mWh per day = approximately 1025 days or 2.8 years.