Integrating Biometrics And Environment Monitoring With Instant Alerts For Enhanced Locker Security

Akshatha Preeth P, Bhoomika B.R., Bhoomika. S, Chaitanya. J, Deekshitha. C

Department of Information Science & Engineering

Global Academy of Technology

Abstract

Bank lockers are a huge issue as the security is plain old. They employ outdated keys, easy passwords, and can't secure valuables from incidents such as fire. In this paper, we examine contemporary security devices in-depth and discover they do not cooperate. To rectify this, we designed a super-secure Smart Locker Security System. It operates on the mighty, compact computer, Raspberry Pi 4, and requires users to undergo five independent identity verifications: face recognition, fingerprint, voice authentication, a physical RFID card, and an individual one-time password (OTP). Even better, it always protects the locker itself with four additional sensors that monitor for fire, smoke, intense shaking, and excessive heat. By combining these nine various security checks with each other, our system builds a solid shield that ensures assets are secure from burglars and calamity.

I. INTRODUCTION

It's amazing that in an era of electronic banking, the security safeguarding our real valuables has not evolved much at all. The legacy systems—plain keys and codes—are too simple to duplicate or pilfer. When a burglar breaks in, or when there is a blaze, the loss is enormous, not only in money, but because individuals lose faith in the bank. We desperately require a dramatic transformation.

Fortunately, we now have the means to do it, such as the Internet of Things (IoT) and low-cost, high-power mini-computers like the Raspberry Pi. These make it simple to create high-tech security.

But the problem is that most researchers only do half a system. They may create a fantastic fingerprint scanner, and another team creates a decent fire alarm, but they never put them together. This creates huge gaps.

Our research is all about plugging those gaps. We are demonstrating a superior model: a nine-layer defense system that addresses both issues simultaneously: preventing the wrong individual from getting in (the identity risk) and keeping the goods from being damaged (the safety risk). We think true security only occurs when all checks collaborate.

II. ARCHITECTURAL RATIONALE AND SYSTEM SYNTHESIS

Our Secure Locker System is based on a straightforward principle: if one check fails, the locker remains locked. It becomes almost impossible for a thief since they need to penetrate nine completely different security barriers at the same time.

The system's brain is the Raspberry Pi 4. It's powerful enough to execute all the sophisticated checks (such as reading a face) and read all the sensors in an instant, which is essential to making everything rapid and secure.

A. The Five Steps to Prove Who You Are

To unlock the locker, you need to go through these five checks of identity, sequentially. If you miss a step, the alarm sounds.

1. The Card You Carry (RFID Tag): You begin by tapping your RFID card. This verifies you possess the correct physical token.

2. The Finger You Use (Fingerprint): Then, you place your finger on the scanner. This check against your fingerprint verifies your physical identity.

3. The Face It Sees (Face Recognition): The camera sees you. It verifies your face, and the system immediately takes your picture and sends it straight to your phone. This ensures you know who is attempting to enter the locker.

4. The Voice It Hears (Voice Authentication): You need to say a secret word or phrase. The system verifies the characteristic sound and pattern of your voice, so it cannot be tricked with a recording.

5. The Code It Needs (OTP): The final verification is a One-Time Password sent to your cell phone. The code always varies, demonstrating that the individual at the locker is the real owner with their phone in hand at this moment.

B. The Four Checks to Safeguard the Items

Our system is always monitoring the locker itself, safeguarding the items from incidents such as fire or physical destruction:

* Smash Alert (Vibration Detector): This detector seeks any severe impacts, forced entry, or heavy vibration on the locker box. It alarms instantly if one attempts to physically break into it.

* Fire/Smoke Detector: This detector continuously sniffs the atmosphere for fire or smoke and provides the quickest possible alert.

* Overheat Alert (Temperature Sensor): This monitors the levels of heat within. A sudden increase might be due to a fire outside or an issue within the locker wall.

III. CRITICAL REVIEW OF PRIOR ART AND IDENTIFIED GAPS

The existing body of research can be segmented into three key domains, all of which, individually, prove insufficient for achieving modern security standards.

A. The Limitations of Unimodal and Dual-Factor Biometrics

Early attempts to modernize security focused on single-factor biometric modalities. Projects centered on fingerprint systems (IJERT authors, 2019) or face recognition (Sharma & Gupta, 2023) offered convenience but were plagued by inherent weaknesses: low resistance to spoofing and high susceptibility to environmental factors (e.g., lighting for facial recognition). The subsequent move to dual-factor systems, often fusing a fingerprint with an RFID card (Harsha & Nandini, 2018), was an improvement but still lacked true redundancy. These systems often suffered from high False Rejection Rates (FRR)—legitimate users being denied access—or, worse, high False Acceptance Rates (FAR), which compromise the system's core integrity. The core failure remains the lack of independent, orthogonal verification layers.

B. Computational Trade-offs and Communication Deficiencies

As researchers sought higher accuracy, complex Deep Learning models became prevalent. While advanced CNNs provided exceptional accuracy for specialized tasks like iris scanning (Peer J, 2023), they introduced significant computational latency and power demands, making them impractical for decentralized, battery- backed IoT devices. Furthermore, many systems relying on complex fusion mechanisms (Brown et al., 2021) often overlooked simple, robust communication protocols. The effectiveness of systems relying on OTP delivery (Vajja et al., 2020) is entirely dependent on the reliability of the communication channel (GSM/Wi-Fi), a factor often treated as a simple input/output step rather than a critical security component. The inability of many prior systems to handle *real-time accountability*—like capturing and broadcasting a perpetrator's image—left users disconnected from the immediate security status.

IV. WHY OLD SECURITY METHODS AREN'T GOOD ENOUGH

We examined how other smart security systems operate and identified three key vulnerabilities that our system addresses.

A. Too Much Trust in Only One or Two Checks

Previous smart systems only did one check (such as just face scanning). If someone managed to find a way around that one check, they easily got in. Even those systems that did two checks (such as a fingerprint and a card) weren't strong enough because they still didn't employ completely different types of security.

B. Too Slow and Too Hard to Use

Most high-tech applications make use of extremely complex programs in order to produce correct results. However, the complex programs are usually so slow and consume so much power that they make the entire system cumbersome to use on a low-end computer like the Raspberry Pi. Additionally, most systems failed to ensure that emergency messages (such as the OTP or fire alarm) would be sent out reliably, resulting in communication lapses.

C. They Only Guard the Lock, Not the Assets

Our greatest mistake that we observed is that most systems concentrate on the lock and don't care about securing the contents inside. A fingerprint verification system is a waste if the contents get damaged by an unexpected fire. Further, most systems lack sensors that can detect an attempt to silently break open the wall rather than the lock. We understood that security should guard the items from all, and not only from individuals attempting to unlock the lock.

V. SYNTHESIS AND THE NOVELTY OF THE INTEGRATED SYSTEM

Our research demonstrates that the most effective security arises from the management of identity checks and security checks as a single unified system.

* Five Various Proofs for Maximum Safety: By having an individual go through five tests that employ totally distinct forms of technology (card, finger, face, voice, and a cell phone code), we make it extremely difficult to hack. This builds the maximum amount of backup security.

* Constantly Looking Out for Trouble: The four sensors are constantly active, so the system is an active protector. When the sensors sense smashing or a fire ignition, the system acts instantly, safeguarding the items before they can be harmed.

* Rapid Proof and Quick Access: The robust Raspberry Pi 4 facilitates all these checks in quick time (approximately 3 seconds). The system logs instantly and sends the images, serving as a wonderful means of catching thieves and leaving instant proof in case anything amiss happens.

VI. CONCLUSION

The security issues with conventional bank lockers are an enormous liability nowadays. Our research confirms that older clever systems are lacking. Our Secure Locker System offers the solution. By effectively constructing a nine-layer defense—five phases to verify identity and four sensors for security—we have established a new, far higher physical security standard. This total, trustworthy system gives banks the smart protector they require to safeguard their most precious assets.

ACKNOWLEDGMENT

We owe a substantial debt of gratitude to the organizations and individuals whose contributions were critical in realizing this vision of next-generation security.

Above all, our honest appreciation goes to our diligent faculty advisors and mentors. Their continued patience, scholarly critiques, and technical expertise were the cornerstone of this entire undertaking, enabling us to tackle the intricacies of integrating five different biometric variables with an IoT real-time platform with confidence.

We thank our academic institution and the Department of Information Science & Engineering sincerely. Provision of required resources, consistent laboratory facilities, and challenging intellectual environments was critical in ensuring the successful deployment and rigorous testing of our nine-factor defense system.

Particular thanks are owed to security professionals and technology collaborators. Their co-operation in contributing actual-world information regarding known vulnerabilities, as well as their embedded system expertise, provided a great counterbalance to our theoretical framework and ensured that our solution confronts real-world security challenges in financial domains today.

Lastly, we value the insightful feedback from our peers and co-workers. Their support and new insights were crucial in honing our strategy, especially in maximizing the system for maximum security and user convenience. This project was motivated by a strong belief in bridging the critical security chasm in physical banking infrastructure using innovative, combined technology.

REFERENCES

[1] Aher, V. A., et al. (2022). Microcontroller-Based Bank Locker Security System.

[2] Brown, R., Bendiab, G., Shiaeles, S., & Ghita, B. (2021). A Novel Multimodal Biometric Authentication System using Machine Learning and Blockchain.

[3] Fernández-Caramés, T. M., et al. (2024). Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications.

[4] Immanuel, J. M. (2019). IoT-Based Face-look and Fingerprint Safe Security System.

[5] IJERT Authors. (2019). Fingerprint-Based Bank Locker Security System.

[6] Jadon, A., et al. (2024). FireNet: A Specialized Lightweight Fire & Smoke Detection Model for Real-Time IoT Applications.

[7] Kumar, A., et al. (2024). Development of Biometric based Intelligent Authentication System for Bank Lockers.

[8] Lakshmi, M., & Prakash, P. (2020). Multimodal Biometric Authentication Using Face and Fingerprint Recognition.

[9] Paneru, N., et al. (2020). IoT-Based Bank Locker Security System.

[10] Peer J. (2023). An Efficient Multi-Factor Authentication Scheme based on CNNs for Securing ATMs over Cognitive-IoT.

[11] Pendke, K., et al. (2020). Smart Locker Security Control System.

[12] Sharma, R., & Gupta, M. (2023). Deep Learning-Based Smart Access Control Using Raspberry Pi.

[13] Singh, A., Dubey, B. K., & Sharma, A. (2025). Microcontroller Based Bank Security System.

[14] S., P., & A., M. (2023). AI-enabled Voice Recognition for Secure Access Systems.

[15] Vajja, V. R., et al. (2020). Advanced Authentication System with Biometric & OTP Integration.

[16] Willie, A., & Bakri, H. (2023). Biometric-Based Multi-Factor Authentication for Digital Banking Security.

[17] G., Harsha, & R., Nandini. (2018). RFID and Biometric Fusion for Locker Access Authentication.

[18] Li, J., et al. (2024). RF-Rhythm: Secure and Usable Two-Factor RFID Authentication