BioGuard
Second defense report

Angel Van den akker and Maria Khvatova

June 3, 2024

Contents

1 Introduction

In today's digital landscape, the need for secure and reliable authentication methods is more critical than ever. As traditional passwords become increasingly vulnerable to breaches, biometric authentication has emerged as a superior alternative, offering enhanced security through the use of unique biological characteristics. This report documents the final phase of our project, focusing on the development and integration of a comprehensive biometric authentication system.

The goal of this project is to create an advanced security solution that leverages fingeprints for user verification. Building on our previous work with fingerprint recognition, we have now created a real application. approach aims to provide a higher level of security and accuracy in user authentication.

Fingerprints, with their unique ridge and valley patterns, have been a reliable form of identification for decades. The distinctiveness of these patterns ensures a high degree of accuracy in verifying an individual's identity. Our project harnesses this reliability, aiming to deliver a biometric authentication system that is both secure and user-friendly.

In this report, we will discuss the methodologies employed in the development of our biometric system, including the design and implementation phases. We will also address the technical challenges we faced during the integration process, such as ensuring compatibility with existing hardware and maintaining user privacy.

.

This final report aims to provide a comprehensive overview of our project's achievements, highlighting the practical implications and fu-

ture potential of biometric systems in enhancing digital security.

2 Background and Related Work

2.1 Biometric Authentication

Biometric authentication is a security process that verifies an individual's identity using unique biological characteristics. Common biometric authentication methods include fingerprint recognition, facial recognition, iris scanning, voice recognition, and even behavioral patterns like typing rhythms. Unlike traditional authentication methods that rely on something the user knows (passwords, PINs) or possesses (security tokens,...), biometric authentication leverages the inherent and unique traits of individuals.

2.2 Types of Biometric Authentication

- **Fingerprint Recognition**: Uses the unique patterns of ridges and valleys on an individual's fingertips.
- **Facial Recognition**: Analyzes facial features such as the distance between the eyes, nose width, and jawline.
- **Iris and Retina Scanning**: Examines the unique patterns in the colored part of the eye (iris) or the pattern of blood vessels in the retina.
- **Voice Recognition**: Identifies individuals based on their unique vocal characteristics.
- **Behavioral Biometrics**: Includes keystroke dynamics, and other behavior-based identification methods.

2.3 Advantages of Biometric Authentication Over Traditional Methods

2.3.1 Enhanced Security

- **Uniqueness**: Biometric traits are unique to each individual, making it difficult for unauthorized users to duplicate or steal.
- **Non-replicability**: Unlike passwords or PINs, biometric data cannot be easily shared, lost, or forgotten, reducing the risk of unauthorized access.

2.3.2 Convenience and User Experience

- **Ease of Use**: Users do not need to remember complex passwords or carry additional hardware like tokens or cards.
- **Speed**: Biometric authentication can be performed quickly, often within seconds, facilitating faster access to systems and devices.

2.3.3 Reduced Administrative Overhead

- **Lower Maintenance**: Eliminates the need for password resets and related support, reducing the burden on IT departments.
- **Cost-Effective**: Over time, biometric systems can be more cost-effective by reducing the expenses associated with password management and security breaches.

2.3.4 Improved Compliance and Accountability

- **Audit Trails**: Biometric systems can provide precise records of who accessed what and when, enhancing accountability and aiding in regulatory compliance.

- **Non-Repudiation**: Because biometric data is unique and directly tied to an individual, it provides a robust method for ensuring that actions cannot be denied by the person who performed them.

2.3.5 Scalability and Flexibility

- **Integration**: Biometric systems can be integrated into various platforms, from mobile devices to large enterprise systems, providing versatile applications across different use cases.
- **Adaptability**: Biometric technologies are continually evolving, with new methods and improvements being developed to enhance security and user experience further.

2.4 Fingerprint Recognition

The use of fingerprints for identification has a long and fascinating history:

Early Use

- **Ancient Civilizations**: Fingerprints were used in ancient Babylon and China for business transactions and to authenticate documents. Clay tablets from Babylon dating back to 2000 BCE bear fingerprints.
- **14th Century Persia**: A Persian book from the 14th century notes the uniqueness of fingerprints as a means of identifying individuals.

Modern Development

- **19th Century**: The modern study of fingerprint recognition began in the 19th century. In 1892, Sir Francis Galton published "Fingerprints" establishing the individuality and permanence of fingerprints.
- **Henry Classification System**: Sir Edward Henry developed a system for classifying fingerprints, which was adopted by law enforcement agencies in the UK and other countries.
- **Early 20th Century**: Fingerprint recognition became a standard practice in forensic science for identifying criminals and verifying identities.

2.4.1 Technical Aspects of Fingerprint Recognition

Fingerprint recognition involves several technical processes to capture, store, and match fingerprints. These processes include:

Fingerprint Acquisition

- **Optical Sensors**: Use light to capture fingerprint images. When a finger is placed on a glass surface, the ridges and valleys reflect light differently, creating a visible pattern.
- **Capacitive Sensors**: Measure the electrical charge between the finger and the sensor. The ridges and valleys create different capacitance values, forming a fingerprint image.
- **Ultrasonic Sensors**: Use high-frequency sound waves to capture the detailed texture of the fingerprint, providing more accurate data even if the finger is dirty or wet.

Image Processing

- **Enhancement**: Fingerprint images are enhanced to improve clarity and contrast. Techniques such as histogram equalization and filtering are used.
- **Segmentation**: The fingerprint area is segmented from the background to focus on the relevant data.
- **Minutiae Extraction**: Key features (minutiae) such as ridge endings and bifurcations are extracted from the enhanced image. These minutiae points are critical for matching fingerprints.

Matching Algorithms

- **Pattern-Based Matching**: Compares the overall patterns and flow of ridges in the fingerprints.
- **Minutiae-Based Matching**: Compares the extracted minutiae points between the stored and input fingerprint images.
- **Hybrid Matching**: Combines both pattern-based and minutiae-based techniques to improve accuracy and reliability.

Template Storage and Security

- **Template Creation**: A fingerprint template is created from the extracted minutiae points. This template is a digital representation of the fingerprint.
- **Storage**: Templates are stored in secure databases. Encryption techniques are employed to protect the templates from unauthorized access.
- **Security Measures**: Advanced security measures, such as liveness detection, are used to prevent spoofing attacks by ensuring that the fingerprint comes from a live finger.

3 System Design and Implementation

3.1 System Architecture

The general workflow of the application is as follows:

1. The application starts and establishes a connection to the SQLite database.
2. The necessary tables are created if they do not exist.
3. When a user attempts to log in, their fingerprint image is read and compared against the stored fingerprint image in the database.
4. If the user does not exist, a new user is created and their fingerprint image is stored.
5. If the user exists and the fingerprint matches, their credentials are retrieved and displayed.

3.1.1 Credential Model

```
#[derive(Debug)]
pub struct Credential {
    pub id: i64,
    pub user_id: i64,
    pub site: String,
    pub site_username: String,
    pub site_password: String,
}
```

3.2 Database Integration

The `database.rs` file manages the connection to the SQLite database and provides functions to interact with the database. The integration of the database into the system involves the following steps:

- **Establishing Connection**: The `establish_connection` function establishes a connection to the SQLite database using the SQLx library. This function uses a hardcoded database URL for simplicity but can be adapted to use environment variables.

```
pub async fn establish_connection() -> SqlitePool {
    let database_url = "sqlite://users.db";
    SqlitePool::connect(&database_url).await.unwrap()
}
```

- **Creating Tables**: The `create_tables` function creates the necessary tables in the database if they do not exist. This includes tables for users and their credentials.
- **Saving Data**: Functions such as `save_user` and `save_credentials` are used to insert data into the database. These functions accept parameters and bind them to the SQL queries to securely insert the data.
- **Retrieving Data**: Functions like `get_user` and `get_credentials` are used to fetch data from the database. These functions execute SQL queries and map the results to the respective data structures.

3.3 Models

The `models.rs` file defines the data structures used in the application.

`Credential`: Represents a user's credential with an ID, user ID, site, site username, and site password.

3.4 Fingerprint Acquisition: Final Review

As we conclude our project, it is crucial to reflect on the progress made in fingerprint acquisition, a fundamental component that has underpinned our work from the beginning. This section will provide a final review of the challenges addressed, the progress achieved, and the future prospects for this critical aspect of our project.

3.4.1 Achievements and Improvements

During the final phase of our project, significant strides have been made in refining the fingerprint acquisition process. Key achievements include:

- **Enhanced Sensor Integration:** We successfully improved the integration of the fingerprint sensor with our C++ codebase, resulting in more reliable and consistent data capture.
- **Feature Extraction Accuracy:** Enhancements in feature extraction techniques have increased the accuracy and reliability of the extracted fingerprint features, crucial for effective biometric matching.

These improvements were built on the foundational work done in the earlier phases, demonstrating our commitment to continuous enhancement.

3.4.2 Addressing Initial Challenges

The challenges identified in the initial and second phases have been systematically addressed throughout the final phase:

- **C++ Adaptation:** Our proficiency in C++ has grown, enabling us to write more efficient and robust code for fingerprint processing.

- **Windows Biometric Framework:** We have deepened our understanding and utilization of the Windows Biometric Framework, ensuring compatibility and leveraging its features for better performance.
- **Library Compatibility:** Continuous updates and testing have ensured our libraries are current and fully compatible with the latest versions, preventing potential integration issues.

By tackling these challenges head-on, we have laid a robust groundwork for the project's success.

3.4.3 Integration and Testing

In this final phase, the focus was on integrating the fingerprint acquisition module with the overall system and conducting extensive testing:

- **System Integration:** The fingerprint acquisition module has been seamlessly integrated with the database and authentication systems, ensuring smooth data flow and operational coherence.
- **Comprehensive Testing:** Rigorous testing was conducted to verify the accuracy, reliability, and performance of the fingerprint acquisition process. Various scenarios were simulated to ensure robustness.
- **User Feedback:** Preliminary user testing provided valuable feedback, leading to minor adjustments and further refinements in the acquisition process.

This phase has confirmed the operational readiness of our fingerprint acquisition system.

3.4.4 Future Prospects

Looking forward, several potential enhancements could be pursued:

- **Advanced Algorithms:** Implementing advanced machine learning algorithms for feature extraction could further enhance accuracy and reliability.
- **Sensor Technology:** Exploring and integrating newer sensor technologies may provide higher resolution and more detailed fingerprint images.

These future considerations will help in keeping the project relevant and up-to-date with technological advancements.

3.4.5 Conclusion

In conclusion, the third phase of our project has been marked by significant progress in the fingerprint acquisition process. The initial challenges were effectively addressed, leading to substantial improvements and a fully integrated system ready for deployment. The groundwork laid in the earlier phases has proven invaluable, providing a solid foundation for our advancements. Moving forward, continuous refinement and embracing new technologies will ensure the sustained success and relevance of our fingerprint acquisition system.

3.5 Minutia Matching

Minutia matching remains a central component in our project, acting as the cornerstone for the comparison of fingerprints during user authentication. Our methodology involves comparing matrices of minutiae between the enrolled user (reference) and the user attempting to authenticate. This process is critical for establishing a reliable biometric authentication system.

The comparison is carried out by employing a threshold value, which is a crucial parameter in determining the acceptance or rejection of a fingerprint match. This threshold serves as a criterion for assessing the similarity between minutiae sets. We perform a pairwise comparison of minutiae, calculating a similarity metric that encompasses spatial distance and orientation difference. Each minutia pair is evaluated against this threshold, and only those exceeding it are considered for further analysis.

The `minutiae matching` function takes references to two fingerprint images, detects minutiae points using the optimized `detect minutiae` function, and compares these points.

The refined minutiae matching algorithm significantly enhances the biometric authentication process in our project. By integrating these improvements, we aim to provide users with a more secure, reliable, and user-friendly authentication method, thereby elevating the overall user experience and security of our system.

4 Technical Challenges

During the development and integration phases of the project, several technical challenges were encountered:

- **Database Connection Management**: Ensuring that the database connection is properly established and managed was challenging. Handling connection pooling and asynchronous database operations required careful attention to avoid issues such as connection leaks and deadlocks.
- **Asynchronous Programming**: Integrating asynchronous programming with the SQLx library and the overall Rust application was complex. Proper use of async/await syntax and error handling mechanisms was crucial to maintain the application's performance and reliability.
- **Error Handling**: Robust error handling for database operations was necessary to ensure the application could gracefully handle various failure scenarios, such as network issues or database unavailability.
- **Data Security**: Storing sensitive information, such as fingerprint images and user credentials, required implementing secure storage practices. Ensuring that data was securely stored and transmitted involved using appropriate encryption and secure coding techniques.
- **User Authentication**: Implementing fingerprint-based authentication required integrating with appropriate libraries and ensuring the accuracy and reliability of fingerprint matching. Handling edge cases, such as partial or corrupted fingerprint images, added to the complexity.

5 Conclusion and Future Work

This project has been an invaluable learning experience, providing us with practical insights into database management, user authentication, and the application of biometric verification systems. Here are some of the key lessons we learned:

- **Database Management:** We gained hands-on experience in designing and managing a SQLite database, including creating tables and handling CRUD (Create, Read, Update, Delete) operations efficiently.
- **Biometric Verification:** Implementing fingerprint verification enhanced our understanding of biometric systems and their potential for secure user authentication.
- **Software Architecture:** Structuring our application using models, database handlers, and a main application loop improved our skills in organizing and maintaining complex software projects.

The project was particularly interesting because it combined several advanced concepts into a cohesive system. The integration of biometric verification with a user credential management system is a compelling application with real-world relevance. It highlighted the importance of security and efficiency in handling sensitive user data.

While we achieved significant milestones, there are several areas where future work can build upon our findings:

- **Model Refinement:** Further refining the fingerprint verification model to improve accuracy and performance, especially in handling edge cases.
- **Integration with Existing Systems:** Exploring how our model can be integrated with existing security systems and technologies to assess its practical applications and scalability.

- **Advanced Techniques:** Investigating advanced techniques, such as machine learning, to enhance the model's predictive capabilities and provide deeper insights.
- **User Experience Improvements:** Focusing on making the system more user-friendly, ensuring that it is accessible to a broader audience, including those without specialized knowledge.

Future research could explore related areas, such as the application of machine learning algorithms for improved biometric verification and collaboration with interdisciplinary teams to address more complex, multifaceted security challenges. Additionally, investigating the potential for real-time application of the system in dynamic environments offers an exciting direction for further study.

In conclusion, this project has provided us with valuable insights and practical experience. By building on these achievements and exploring the outlined future work, we can continue to advance our understanding and contribute meaningful solutions to the field of biometric authentication and secure data management.