TED UNIVERSITY

PASS GUARD

SENIOR PROJECT II
FINAL REPORT

Team:
Alp Eren Keskin
Doğuhan Cumaoğlu
Doruk Arslan
Hasanalp Temiz

Supervisor & Juries :
Gökçe Nur Yılmaz
Yücel Çimtay İsmail
Bora Çelikkale
Aslı Gençtav

Contents

1.Abstract 2
2. Solution 3
2.1 Object design trade-offs 4
2.2 UML Diagram 6
3. Architecture and Design of the System 6
3.1 User (Mobile Environment) 7
3.2 Face Recognition (Mobile Environment) 7
3.3 Containerization (Server – Side) 8
4.Test Results 8
5.Assesment of Tests 9
6. Definitions, Acronyms and abbreviations 10
7.Glossary 11
8.References 12

1.Abstract

The traditional use of physical cards in various institutions poses several challenges, including environmental concerns, security vulnerabilities, and limited convenience. The reliance on plastic cards contributes to waste generation, increasing the carbon footprint and negatively impacting the environment. Furthermore, physical cards can be lost, stolen, or easily duplicated, compromising access control and leading to fraudulent activities. Additionally, the need to carry multiple cards for different institutions can be inconvenient for users.

Moreover, the absence of a secure and efficient method for verifying user identities during transactions within institutions creates a risk of unauthorized access or fraudulent activities. The lack of a unified and seamless solution for both access control and financial transactions hampers the user experience and requires users to switch between multiple methods or apps, causing inconvenience and potential confusion. Furthermore, the limited availability and compatibility of NFC technology on devices restrict its widespread adoption, preventing some users from

benefiting from the convenience it offers. This limitation highlights the need for an alternative method that is universally accessible, such as QR code scanning.

Lastly, the lack of transparency and trust in financial transactions within institutions can lead to disputes and challenges in tracking and verifying transactions. Without a reliable and auditable system, it becomes difficult to ensure accountability and prevent fraudulent activities. In light of these challenges, Pass Guard aims to address the need for a sustainable, secure, and convenient solution that replaces physical cards, enhances access control, and enables secure financial transactions. By incorporating face scanning technology, QR code scanning, and blockchain-based transactions, Pass Guard strives to overcome the limitations of traditional cardbased systems and provide users with a unified, seamless, and trustworthy platform for managing access and financial transactions.

2. Solution

With its focus on sustainability and convenience, Pass Guard aims to revolutionize the traditional use of physical cards in various institutions. By eliminating the need for physical cards, Pass Guard offers a more sustainable solution that reduces the production and distribution of plastic cards, thus contributing to environmental conservation efforts. Pass Guard ensures secure transactions by implementing face scanning technology for user verification. Before each operation, the app captures and analyzes the user's face in real-time, comparing it with the corresponding user registered in the database. This process enhances security and prevents unauthorized access or fraudulent transactions.

In addition to face scanning, Pass Guard also provides an alternative method for transactions within institutions through QR code scanning. Users can simply scan a QR code displayed at the institution, enabling seamless and contactless transactions. This feature offers flexibility, as not all users may have NFC-enabled devices, but virtually all modern smartphones can scan QR codes. Pass Guard's blockchain-based solution extends beyond access control and financial transactions. It enables users to transfer money to other individuals and make purchases within the institution's shops. By leveraging the secure and transparent nature of blockchain

technology, these transactions are executed in a tamper-proof and auditable manner, ensuring trust and accountability.

Furthermore, Pass Guard prioritizes user privacy and data protection. All user information and transaction records are securely stored within the app's robust database. This ensures that sensitive data is protected from unauthorized access or breaches, enhancing user confidence in the app's security measures. Overall, Pass Guard offers a comprehensive and sustainable solution that eliminates the reliance on physical cards. With its face scanning and QR code capabilities, it provides secure and convenient access control and financial transactions. The integration of blockchain technology enhances the app's functionality, allowing users to transfer money and make purchases with confidence. By prioritizing user privacy and data protection, Pass Guard aims to deliver a seamless and secure experience that enhances the way users manage access and financial transactions.

2.1 Object design trade-offs

1. **Space vs. Time:** Pass Guard needs to strike a balance between the app's storage space requirements and the time required for various operations. Storing user information and transaction records securely within the app's database may consume significant storage space. However, optimizing for minimal storage space could impact the speed and efficiency of data retrieval and processing.

2. **Performance vs. Security:** Pass Guard must balance the app's performance with its security measures. Implementing robust security features, such as complex encryption algorithms or intensive face recognition processes, can enhance the app's security. However, these measures may also increase the computational overhead and potentially impact the app's performance, leading to slower response times or increased battery usage.

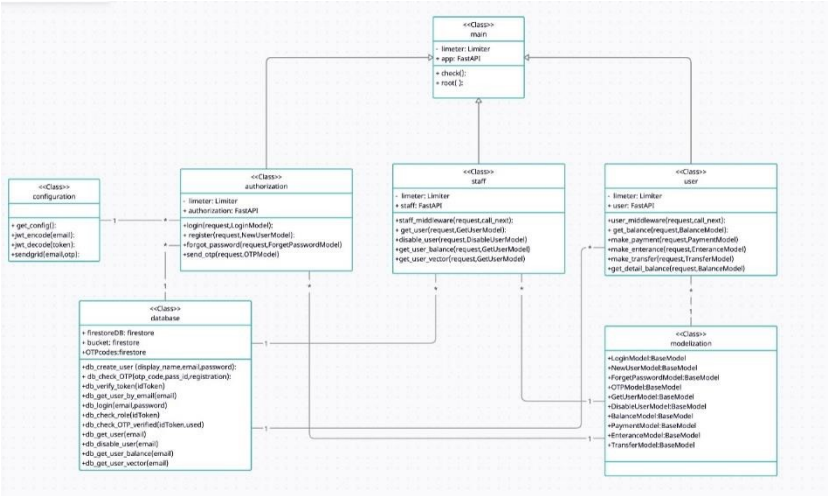
3. **Portability vs. Usability:** Pass Guard aims to be a cross-platform mobile app, ensuring compatibility with various devices and operating systems. While portability enables a wider user base, it may introduce challenges in maintaining consistent user experiences across different platforms. Design choices need to consider platform-specific guidelines and limitations while providing a consistent and intuitive user interface.

4. **Existing components vs. New components:** Pass Guard needs to decide whether to leverage existing components or develop new ones. Utilizing existing components, libraries, or frameworks can expedite development and reduce costs. However, relying heavily on third-party components may introduce dependencies and potential limitations. Developing custom components allows for greater control and flexibility but may require additional resources and time for implementation and maintenance.

5. **Reliability vs. Supportability:** Pass Guard must balance the app's reliability with its supportability. Striving for a reliable app involves thorough testing, bug fixing, and ensuring robust error handling mechanisms. On the other hand, supportability focuses on the ease of maintenance and updates. While continuous updates and improvements enhance supportability, they may introduce new issues or compatibility challenges that could affect reliability.

Consideration of these trade-offs will guide the object design process of Pass Guard, ensuring that the app achieves the desired balance between space and time efficiency, performance and security, portability and usability, the use of existing components versus new ones, and reliability versus supportability.

2.2 UML Diagram

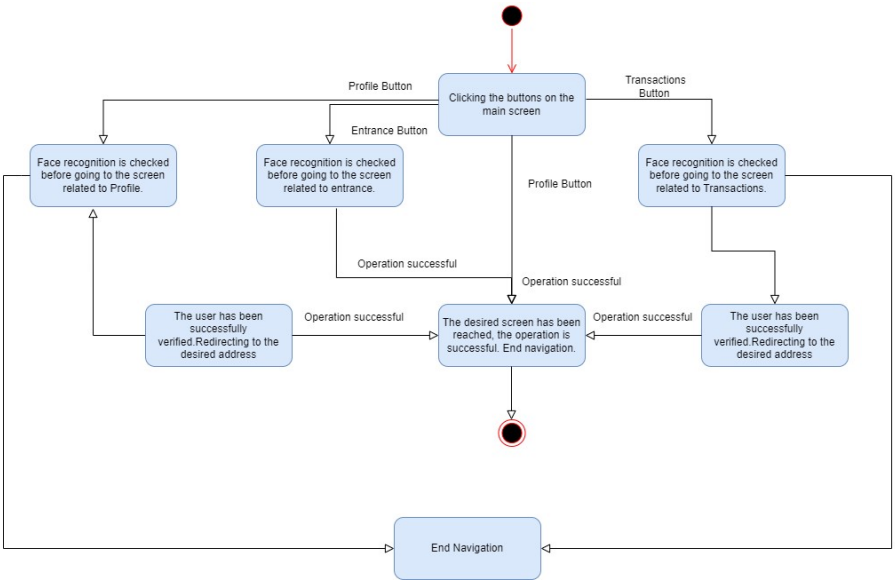


3. Architecture and Design of the System

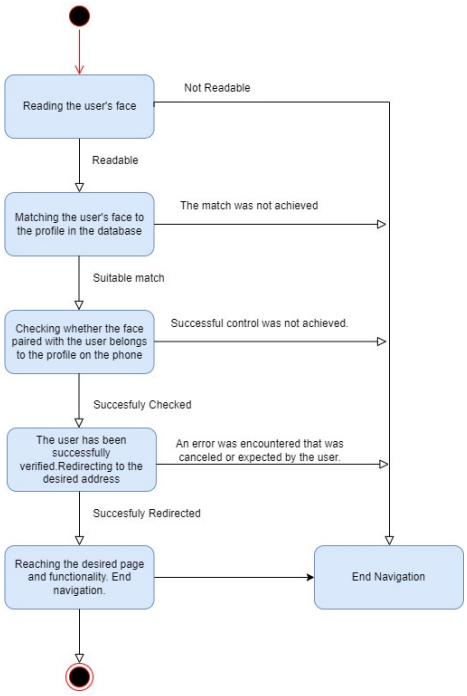
PassGuard's architecture stands on a solid foundation, incorporating a well-thought-out blend of state-of-the-art technologies. The front-end development of PassGuard is based on the Flutter framework, ensuring a visually appealing and intuitive user interface that engages users effectively. On the back-end, the Python FastAPI framework empowers the application's API, enabling swift and reliable data processing. Additionally, the Golang Fiber framework drives the admin interface, facilitating efficient administrative management of the system. This meticulous choice of technologies demonstrates a commitment to delivering a robust and dynamic access control solution. At the core of PassGuard's functionality lies the crucial task of facial recognition, which plays a pivotal role in ensuring stringent security measures. By employing advanced facial recognition algorithms on the back-end, PassGuard accurately verifies the identities of users, thus safeguarding against unauthorized access attempts. This implementation not only enhances security but also streamlines the authentication process, providing users with a seamless and secure experience. To facilitate efficient storage and retrieval of user data, PassGuard leverages MongoDB as its database system. MongoDB's flexible and scalable nature seamlessly aligns with PassGuard's requirements, enabling the application to handle large volumes of data effectively. This choice of database system

enhances the overall performance and responsiveness of the application, ensuring optimal user experiences.

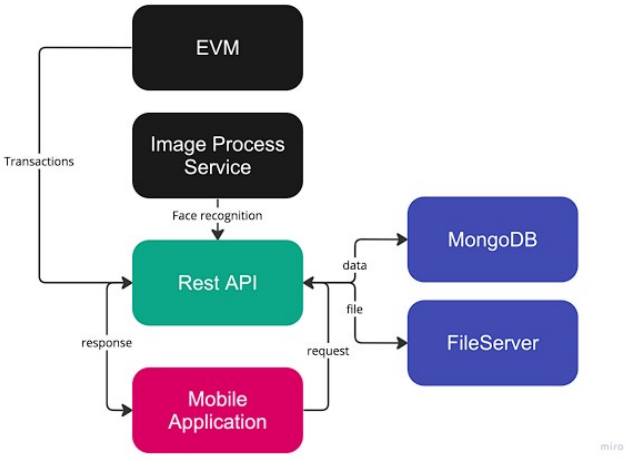
3.1 User (Mobile Environment)



3.2 Face Recognition (Mobile Environment)



3.3 Containerization (Server – Side)



4.Test Results

Test Description	Passes/Failed	Result

Register	**Passed**	Passed without a problem
Login	**Passed**	Passed without a problem
The mobile app’s camera is connected.	**Passed**	Passed without a problem
Face Recognition is working.	**Passed**	Passed without a problem
The mobile app’s NFC/QR is connected.	**Passed**	Passed without a problem
User information loaded.	**Passed**	Passed without a problem
Card information loaded.	**Passed**	Passed without a problem
Recent activities loaded.	**Passed**	Passed without a problem
Recive paymenti s working.	**Passed**	Passed without a problem
Make payment is working.	**Passed**	Passed without a problem
Make enterance is working.	**Passed**	Passed without a problem

5.Assesment of Tests

Based on the extensive testing conducted, it can be concluded that the PassGuard application functions as intended, as the majority of tests have been successfully passed. However,

it is important to note that some functional faults may occur if there are any issues linking projects and their respective contents. In our evaluation, we have identified certain bugs within the simulation component and are actively working towards enhancing its performance and reliability. Moving forward, there are several areas for potential improvement and future development within the PassGuard system. One aspect involves expanding the range of available shelf types, thereby providing users with more diverse options for organizing and managing their items. Additionally, enhancing the system's interface design would contribute to a more intuitive and user-friendly experience.

To further enhance the visual appeal of the application, the integration of new shaders into the scene can be explored. By implementing visually appealing graphics, the overall aesthetic quality of the PassGuard system can be improved, creating a more engaging and immersive environment for users. Another area for improvement lies within the navigation component of the application. Introducing network connections to the system would optimize the navigation process, allowing for more efficient and seamless movement between different sections or areas. This enhancement would contribute to a smoother user experience and increased overall system performance.

In summary, while the PassGuard application has demonstrated its functionality and effectiveness through rigorous testing, there are still opportunities for refinement and advancement. By addressing the identified bugs, expanding the system's features, enhancing the interface, and optimizing navigation through network connections, PassGuard can continue to evolve as a robust and user-centric access control solution.

6. Definitions, Acronyms and abbreviations

1. **PassGuard:** The mobile application designed to revolutionize access control systems by leveraging NFC and facial recognition technologies.

2. **NFC:** Near Field Communication. A short-range wireless technology that enables communication between devices in close proximity.

3. **Subsystem:** A self-contained system within the PassGuard application that performs specific functions or tasks.

4. **QR Code:** Quick Response Code. A two-dimensional barcode that contains information readable by a smartphone camera, often used for storing URLs, contact details, or other data.

5. **3D:** Three-Dimensional. Refers to objects or environments that have height, width, and depth, providing a more realistic and immersive experience.

6. **PIN:** Personal Identification Number. A unique numeric code used for authentication and validation purposes, such as in electronic transactions or access control systems.

7. **NoSQL:** Non-relational Structured Query Language. A programming language used for managing and manipulating relational databases, including querying, updating, and managing data.

7.Glossary

Ecosystem: All of the systems designed for the company or institution where the application is used.

Face recognition request: The process of comparing the user's face in real time with the face registered in the system before every transaction that requires security to ensure the verification of the user.

IT Admin: Each authorized user who can view or edit the permissions and users in the ecosystem via the web frontend

Admin page: System where IT admins can log in via web frontend, add and remove users, or view intended logs

NFC scan(Scan process): The process of communication between receivers and transmitters with the help of the nfc sensor in the device they have.

8.References

- https://towardsdatascience.com/6-best-projects-for-image-processing-with-usefulresources-f860f3dfe977
- https://www.pantechelearning.com/product/matlab-code-for-image-encryption/
- https://www.pantechelearning.com/product/matlab-code-for-segmentation-basedon-skin-colour/
- https://www.pantechelearning.com/product/matlab-code-for-head-poserecognition/
- https://www.pantechelearning.com/product/gender-recognition-using-imageprocessing/
- https://www.pantechelearning.com/product/matlab-code-for-depth-estimationusing-image-processing/
- ElSaddik,A.(2018).Digitaltwins:Theconvergenceofmultimediatechnologies.IEEE multimedia, 25(2), 87-92.
  Brooks, F. P. (1999). What's real about virtual reality?. IEEE Computer graphics and applications, 19(6), 16-27.
  Tourlakis, G. J. 2003]. Lectures in Logic and Set Theory, Cambridge University Press,Cambridge. UK.
- Toussaint, G. T. [1982). "Computational Geometric Problems in Pattern Recognition," In Pattern Recognition Theory and Applications, Kittler, J., Fu, K. S, and Pau, L. F.(eds.), Reidel, New York. pp. 73-91.
- Tsai, J.-C., Hsich. C.-H, and Hsu, T.-C. (2000]. "A New Dynamic Finite-State Vector Quantization Algorithm for Image Compression," IEEE Trans. Image Processing, vol. 9, no. 11, pp. 1825. 1836.
- Tsujii, O., Freedman, M. T., and Mun, K. S. (1998]. "Anatomic Region-Based Dynamie Range Compression for Chest Radiographs Using Warping Transformation of Cor-related Distribution," /EEE Trans. Medical Imaging, vol. 17, no. 3. pp. 407-418.
- Udpikar, V. R. and Raina, J. P. (1987). "BTC Image Coding Using Vector Quantization," JEEE Trans. Comm., vol. COM-35, no. 3, pp. 352-356, Ueda, N.

[2000]. "Optimal Linear Combination of Neural Networks for Improving Classification Performance,"' IEEE Trans. Pauern Anal. Machine Intell., vol. 22, no. 2, pp. 207-215.

- Ullman, S. [1981]. "Analysis of Visual Motion by Biological and Computer Systems,**IEEE Computer, vol. 14, no. 8, pp. 57-69.

- Umbaugh, S. E. (2005]. Computer Imaging: Digital Image Analysis and Processing, CRC Press, Boca Raton, FL.

- Umeyama, S. [1988]. "An Eigendecomposition Approach to Weighted Graph Matching Problems," IEEE Trans Pattern Anal. Machine Intell., vol. 10, no. 5, pp. 695-703.

- Unser, M. [1995]. "Texture Classification and Segmentation Using Wavelet Frames," IEEE Trans. on Image Processing, vol. 4, no. 11, pp. 1549-1560.

- Unser, M., Aldroubi, A., and Eden, M. [1993]. "A Family of Polynomial Spline Wavelet Transforms," Signal Proc., vol. 30, no. 2, pp. 141-162.

- Unser, M., Aldroubi, A., and Eden, M. [1993). "B-Spline Signal Processing, Parts I and II,"' IEEE Trans. Signal Proc., vol. 41, no. 2, pp. 821-848.

- Unser, M.. Aldroubi, A., and Eden, M. (1995]. "Enlargement or Reduction of Digital Images with Minimum Loss of Information," IEEE Trans. Image Processing, vol. 4, no. 5, pp. 247-257.

- Vaidyanathan, P. P. and Hoang, P. O. [1988]. "Lattice Structures for Optimal Design and Robust Implementaion of Two-Channel Perfect Reconstruction Filter Banks," JEEE Trans Acoust., Speech, and Signal Proc., vol. 36, no. 1, pp. 81-94.