

Fingerprint Authentication Project

**Name: Ben Frost**

**Student ID: S246228**

**Submission Date: [Date]**

**Supervisor: Dr Kakia Chatsiou**

Declaration

All content quoted in this paper from other authors publications have been specifically acknowledged by clear cross-referencing to author, work and page(s). Any illustrations that are not the work of the author of this paper have been used with the explicit permission of the originator and are specifically acknowledged. I understand that failure to do this could be considered plagiarism and will be considered grounds for failure in this project and the degree as a whole.

Ben Frost

Abstract

[The abstract briefly summarises your project. It should provide a concise description of the need for such a project, what this project intends to achieve (aims) and the results. The abstract is usually the last chapter of the report to be completed once you have an overview of the whole project. The abstract should be 6 to 12 sentences. For examples, consult a journal article to see how an abstract is constructed.]

**Keywords**: [Add about six keywords which would help a search engine find your report]

Acknowledgements

I would like to give thanks to my supervisor, Kakia, for the support I received. The scheduled meetings, for updates on this dissertation project, helped immeasurably. Due to the support, solutions to my problems were concluded very quickly. This allowed me to overcome hurdles as I had someone to talk to about the struggles, as well what has been tried and failed.

[This chapter is an opportunity to acknowledge anyone who has made a contribution to the project. At a minimum, you should acknowledge your supervisor. Keep this chapter short, one paragraph is usually enough.]

Table of Contents

[Declaration i](#_Toc194928189)

[Abstract ii](#_Toc194928190)

[Acknowledgements iii](#_Toc194928191)

[Table of Contents 1](#_Toc194928192)

[List of Figures 3](#_Toc194928193)

[List of Tables 4](#_Toc194928194)

[List of Abbreviations 5](#_Toc194928195)

[1 Project Introduction, Motivations and Background 6](#_Toc194928196)

[1.1 Relevance to Security Implementation 6](#_Toc194928197)

[1.2 Project Aim and Expected Outcome 7](#_Toc194928198)

[2 Literature Review and/or Technology Review (other systems like it that use fingerprint scanners, distributed systems etc) 8](#_Toc194928199)

[2.1 Authentication 8](#_Toc194928200)

[2.2 Data Security 9](#_Toc194928201)

[2.3 Biometric Techniques 9](#_Toc194928202)

[2.4 Existing Technology 11](#_Toc194928203)

[3 Project Plan and Methodologies (talk about how I done my project, breaking up tasks etc, agile waterfall, rapid prototyping) 12](#_Toc194928204)

[3.1 Project plans 13](#_Toc194928205)

[3.2 Methodologies 13](#_Toc194928206)

[3.2.1 Hardware 14](#_Toc194928207)

[3.2.2 Software 14](#_Toc194928208)

[4 System Analysis and Requirements 15](#_Toc194928209)

[5 System Design 19](#_Toc194928210)

[6 Implementation + progression (talk implementation of hardware/software) 20](#_Toc194928211)

[7 Testing and Evaluation 23](#_Toc194928212)

[7.1 Tests 23](#_Toc194928213)

[7.1.1 Capturing Fingerprint 23](#_Toc194928214)

[7.1.2 Storing Fingerprint 23](#_Toc194928215)

[7.1.3 Verifying Fingerprint 23](#_Toc194928216)

[7.1.4 Deleting Fingerprint 23](#_Toc194928217)

[8 Maintenance and Deployment 24](#_Toc194928218)

[9 Results and Discussion 25](#_Toc194928219)

[10 Future Work 26](#_Toc194928220)

[11 References 27](#_Toc194928221)

[12 Bibliography 29](#_Toc194928222)

[13 Appendix A 30](#_Toc194928223)

[To update the table of contents, make sure you have formatted any chapter headings using one of the styles embedded in this document. Then place the cursor anywhere in the Table of Contents and press F9. Then select UPDATE THE ENTIRE TABLE and press OK.]

List of Figures

[Figure 1: Easy Colours 4](#_Toc143255913)

[To add entries to this list:

* insert/create the figure, then place the cursor in a newline below the figure. In the REFERENCES menu, select INSERT CAPTION.
* In the caption window, enter a name for the figure. I recommend that you add a colon then a space character before the name as the table number will automatically be inserted before you caption, for example if you want the name of the caption to be ‘Population Growth’ enter ‘: Population Growth’, Word will then place the caption “Figure 2: Population Growth’ into the document.]
* In the LABEL option choose FIGURE, then click OK. This places the caption below the figure.
* To update the LIST OF FIGURES, place the cursor anywhere in the List of Figures and press F9. Then select UPDATE THE ENTIRE TABLE and press OK.

List of Tables

[Table 1test 3](#_Toc143256679)

[Table 2: Test Table 1 6](#_Toc143256680)

[To add entries to this list:

* insert/create the figure, then place the cursor in a newline below the figure. In the REFERENCES menu, select INSERT CAPTION.
* In the caption window, enter a name for the figure. I recommend that you add a colon then a space character before the name as the table number will automatically be inserted before you caption, for example if you want the name of the caption to be ‘Original Data’ enter ‘: Original Data’, Word will then place the caption “Table 2: Original Data’ into the document.]
* In the LABEL option choose FIGURE, then click OK. This places the caption below the figure.
* To update the LIST OF FIGURES, place the cursor anywhere in the List of Figures and press F9. Then select UPDATE THE ENTIRE TABLE and press OK.

List of Abbreviations

[Place abbreviations in alphabetical order.]

# Project Introduction, Motivations and Background

Two foundational pillars of cybersecurity are authentication and authorization, alongside the principles of the CIA triad: confidentiality, integrity, and accessibility. According to the National Institute of Standards and Technology (NIST) in standard 1800-25A, confidentiality ensures that stored data remains private and accessible only to authorised personnel. Integrity guarantees that the data remains unaltered and is safeguarded against destruction. Accessibility ensures that authorised parties can reliably and consistently access the data when required (Elkstrom *et al.,* 2020).

Authentication and authorisation are critical components of access control, which involves granting individuals or accounts the rights to access systems or resources. Authentication verifies the identity of a person or entity, typically through mechanisms such as passwords. Authorization determines whether the authenticated individual has the necessary permissions to access a resource. Authentication methods fall into three main categories: what you know (e.g., passwords), what you own (e.g., keyless fobs), and what you have (e.g., biometrics) (Idrus *et al.,* 2013).

## Relevance to Security Implementation

The importance of these concepts lies in their role in maintaining robust access control mechanisms. However, traditional methods like passwords can be forgotten or stolen, key fobs can be lost or cloned, and even biometrics can be subject to replication. This project explores the use of biometrics, specifically fingerprints, as a more secure alternative for authentication systems. Unlike passwords or fobs, biometrics are inherently tied to the individual and are difficult to lose or replicate. The improved safety aspect comes from using two prints from two different fingers as the password. This then means that there are 9,072 different combinations you can have with 10 prints. Although less combinations than a password, fingerprints cannot be forgotten or guessed by a threat actor.

## Project Aim and Expected Outcome

The project aims to design and implement a biometric authentication system utilizing a fingerprint scanner capable of recognizing multiple fingerprints during the login process. The implementation will rely on off-the-shelf hardware and open-source software to ensure accessibility and reproducibility. The expected outcome will demonstrate the viability of biometrics as a highly secure solution for systems requiring stringent security measures. The project emphasizes the operational functionality of biometrics rather than focusing on extensive software development. Wouldn’t it be far easier if you could just walk into a bank or an establishment and withdraw/pay with the fingers on your hand? The main issue, that the project is aiming to solve, is how unreliable outdated forms of banking can be. Cards are easily lost or stolen, leading to the potential misuse by strangers who either find it, or have stolen it. The project has the idea that biometrics can be used for banking transactions and, could potentially reduce security risks along with the added benefit of not having the burden of remembering cards and pin codes/passwords.

Here, you provide the reader with general background knowledge to understand your project. Assume the reader has some general knowledge of computing but is not familiar with the specific topic of the project. Provide a *brief* description of key concepts and/or theories, enough information for the reader to understand how your project fits into the wider topic. Aim to provide a general overview related to your project and then go into lower level detail in the Literature Review chapter.

Use this background information to bring the conversation to appoint where you identify a problem or need which your project will satisfy. This becomes the *motivation* for your project. The previous paragraphs should all help work towards you stating this motivation. If a section of text is not directly helping you work towards this motivation then ask yourself if you really need that text in the report, if the answer is no, remove it.

Once the motivation is stated, next clearly state the benefits of the project (who or what will benefit, how will they benefit). If you believe this project will do something which has not been done before (the approach is ‘novel’) then clearly state the novelty. This is also a good place to clarify what the final outcome will be. Will it be a software tool, guidelines, information, recommendations. You should use words like *contribute*, *benefit*, *advantageous*, and possibly *novel.* Be careful with the term ‘novel’, you have to be very sure your solution is unique. You could leave yourself open to criticism if you use that term but do not do enough research and fail to discover that someone has already provided a similar solution!

# Literature Review and/or Technology Review (other systems like it that use fingerprint scanners, distributed systems etc)

Through this review, we will discuss the importance of data protection. Using different formats of securing information, as well as authentication, authorisation, and biometric techniques. Using existing literature, this review aims to compare different literature and findings, to evaluate their effectiveness in system authentication and security. This will help decide what the best approach for biometric authentication methods and data storing are.

## Authentication

Authentication is a must for secure design of systems. Policies vary greatly across different systems. For example, some systems may optimise the use of a default deny policy. This policy means that the system denies them at every instance. The user must almost have to prove why they deserve to gain access, using standard methods such as a username and password to gain authentication and authorisation. Authentication systems as a concept, answer the questions of who is the person trying to gain access? and are they who they say they are? Idrus et al (2013). The standard of authentication currently, is the use of two step authentication. This is where the user has another piece of information to prove they are who they say they are. They are based on three different factors for such a system to work effectively. These are such factors as knowledge, possession and inherence. These are simply put as something they know, something they own or something they have. Passwords are something they know, key fob is something they own and fingerprint is something they have Velasquez et al (2018). Keeping this as robust as possible is vital to keeping data secure.

## Data Security

It is important for any sensitive data to be kept hidden from anyone, especially from someone that may misuse it. An established way to achieve this is to encrypt data at rest, as said by Shingari and mago (2024) in their paper on the importance of encryption for the medical sectors data, it is proven, that following strict security protocols lowers the threat of a data breach/leak. Later, they go on to mention that data encryption is a vital part of prevention. The kinds of threat prevention are unauthorised access, use, and disclosure of sensitive data. This means that encryption is a good standard to use for the project, to store the highly sensitive print data. However, another option that is to be considered for storing the data would be the use of a hash function. As described by kamal, P (2019) in security of password hashing, the hash function is used to store the plaintext password without being able to see what the password really is, as it has been hashed by an algorithm and isn’t readable to humans. It does this by storing the password with a fixed length output, regardless of the input size. By doing this when a user needs to be authenticated, their entered password is hashed by the same algorithm and compared to the stored hash. If they’re the same, then it has a matched password and the user gains access. This is also a good method to use and has become a standard, along with other techniques, to store passwords for standard methods as well as biometric authentication techniques.

## Biometric Techniques

Biometric authentication has been a developing technology for decades. As discussed in the publishment, an introduction to evaluating biometric systems, Phillips et al (2000), there are many forms and use cases for biometrics. They discuss the main and most common biometrics, such as facial, fingerprint and vocal. They also discuss about how useful biometrics are. Even to the extent of potentially using fingerprints to sign key pairs for encryption. This supports the idea of biometrics being an ideal replacement for the generic alpha-numeral standard for passwords. Although some systems, particularly the facial recognition, has its flaws. Currently some of the issues with this system found in the same report, include lighting conditions. Some faults have been noticed with the performance under light differences. Faults with fingerprint biometrics systems found by M.H.Ali et al (2016) is the type of scanning that you would choose. There is the payoff that having a very fast system will have a lower accuracy rate. Which means that inversely, to have a better accuracy rate it is more robust to make it slower. This is something that needs to be considered when designing the system, as the project is based for finances, security is of upmost importance. As backed by the journal from Unar et al (2014) the methods have different subsets of biometrics. Having various means of biometric authentication opens the use of biometric properties, this is likely to decrease attack surface for any one person. For example, if your online banking has fingerprint technology but your social media uses retina scanning, if an attacker gains access to your social media, they wouldn’t be able to get your bank account as they would be different formats. In the past, this would be slightly different, as although the advice is to have different passwords for everything, no one can remember all their passwords. This means that repeat passwords are very often used.

A diagram of a biometrical structure

AI-generated content may be incorrect.



Figure x: Biometric Types

## Existing Technology

In the modern day, fingerprint scanners are in the everyday smartphone. They are used not only for accessing your phone, but they are also used for payments and logging into different applications. There are many stipulations with fingerprint scanners integrated in mobile devices. They must consider the position of the scan, normal fingerprint scanners being mounted a specific way, they are likely to catch the print image the same way. Whereas on a mobile device, the scanner can be in many different positions. The scanner would also have different conditions to deal with, such as moisture differences and lighting differences Saavedra et al (2016). Through the paper they discuss a study, in this study it was found that there is a limit to the size of the fingerprint imaging size. The lowest size recommended for a fingerprint image is 320x320 pixels, as less than this recommended size found considerable degrading in matching performance. In another research paper, image quality plays a vital role in the success rate of the matching process. To enforce the highest standards, a high quality image should be taken for the base enrolment image. This then allows any image used for matching to be lower quality and still have a high success on matching Ordani and McCabe (2009).

A Literature Review chapter is required. A Technology Review chapter is optional based on the nature of the project and may be separate or combined with the literature review.

Now that you have provided a general background and identified a problem and solution (motivation), you can focus in on the detail required to understand the specifics of your project. You do this by reviewing the literature specific to your proposed solution which may involve discussing relevant software, API’s, algorithms, related project etc. You should aim to compare and contrast different approaches, identify strengths and weaknesses and keep in mind the phrase ‘critical evaluation’, as your review the literature.

Have a look at the introduction section of academic journal papers. These tend to act as an introduction and literature review combined, although we recommend you split these out to two chapters in your report. Note the high frequency of citations compared to other sections. As the word count is limited in a journal paper, rather than explaining every concept or previous piece of work by other authors, the main findings or theories from each paper are often summarised in a sentence with an accompanying citation to allow the reader to read more about if they wish to, for example “Ross (2014) generated 3d terrain with graph transformation, however, Jones (2016) identified this approach lacked the ability to generate vertical concave surfaces”. Related work is often identified by providing a group of citations, for example: “Several authors have demonstrated the effectiveness of shape grammars in procedurally generating buildings (Highgate 2012, Smith & James, 2010 & Williams 2011)”. Do not just throw in lots of different sources in an unrelated list of citations, you still need to demonstrate your understanding of how these sources relate to your proposed solution. Do not assume more citations equals more marks, it does not!

Getting the balance between breadth and depth can be challenging, there are not strict rules on this. Reviewing 2 sources in detail is not sufficient. This is not extensive research.

You should aim to have the majority of citations from academic peer reviewed journal and conference papers. Journal/conference papers are preferred over books which are preferred over websites. Some technical information will only be available on website which is understandable. You should aim to have an introduction main body and summary sections within the literature review. These do not need to be shown as specific section headings, just to help with the structure. Do not just review one source after the other. Compare and contrast sources, join the discussion of various sources so they flow together to finally arrive at a justification for your chosen solution.

# Project Plan and Methodologies (talk about how I done my project, breaking up tasks etc, agile waterfall, rapid prototyping)

Provide a brief overview of the project management methodology and tools you have selected (agile/waterfall, MoSCoW prioritisation, critical path analysis etc.). Make it clear why you are using the selected approaches. Explaining why you rejected other techniques can help with the justification of your choices.

Provide an initial plan (Gantt chart or other) which you created at the start of the project. Provide an update final version of this plan in the review 9 Results and Discussion of the report to show how the plan changed.

## Project plans

During the creation of the project, the agile-waterfall hybrid development process was adopted. This method suited the project progression, as it involves incremental improvements over the lifecycle of the process. I found it more beneficial to use than either waterfall of agile on their own. This helps with making robust requirements but then also the added benefit of being able to compartmentalise sections of the project and ensuring that each part works independent of each other before trying to bring it all together but allowing flexibility with creation process. This ensures that any faults within each section is fixed. This means that rather than having a large subset of, for example, code to run through every time there is a fault, it limits the possibilities as to where and error is occurring from. For example, an extra step in the fingerprint scanning function was required, after it was thought that scanning the print function was finished, to improve the print image quality. Adding the extra efforts of the MoSCoW method for requirements prioritisation meant I had a clear outlined goal of the essential parts for the project. This enabled me to stay on task with greater efficiency and keep the focus on topic and not on adding to the workload needlessly.

A screenshot of a computer program

Description automatically generated

## Methodologies

In this section I will outline the methodology that I followed, only depicting the information that was found to be useful and the parts of the process that were successful. This shows how the project can be made from start to finish without any faults, allowing replication in a successful manor and time frame.

### Hardware

The set up of the Arduino hardware was a simple task. The hardware included the set-up instruction in the form of a website link, to a file of the specifications and the instructions on how to set it up. The useable cables that this project requires from the Arduino are the black one (1) which is ground, the red one (4) which is power in using 5V, the white one (2) which is the serial in and the green one (3) which is serial out. The use of the two serial wires enables the Arduino to communicate with hardware or other software that Is being used to send and receive commands and data. In this case it is python being used to send and receive data with the Arduino (see figure for graphical representation of set up, also a link to the entire pdf).

[A white background with black text

Description automatically generated](https://www.farnell.com/datasheets/3216194.pdf)

Figure x: Datasheet Wire Information

### Software

The interface for the scanner project needed to be a friendly and useable language. Python was therefore used for this purpose, as it has a lot of support for software development capabilities. The added benefit of choosing python for this use case over java, for example, is that pythons support for fingerprint scanning projects is larger. They have specific libraries to help in this project. It has a very simple serial connection creation, for the communication between scanner and interface, as well as being able to create a GUI, if necessary.

# System Analysis and Requirements

To ensure timely delivery of the project outputs and The MoSCoW prioritisation method is used to define the prioritisation of features for the application. The method splits requirements into “must haves” (M), “should haves” (S), “could haves” (C) and “wish to haves” (W) helping developers with prioritising these towards a minimum viable product (MVP). Requirements will also be split and organised using the functional vs non-functional methodology: as Kurtanovic and Maalej said, Functional requirements are system functionalities, things that will be interacted with such as, a way to add users. Non-functional requirements are system properties, things that happen in the background such as security for the biometric passwords (Kurtanovic and Maalej, 2017).

|  |  |  |  |
| --- | --- | --- | --- |
| Mo | S | Co | W |

|  |  |  |
| --- | --- | --- |
| Functional Feature | Description | priority |
| User authentication | Using some form of biometrics to log into the ‘banking app’. | Mo |
| Add users from an admin login | Have a way to add users to database to be able to authenticate. | Mo |
| a banking home page | Make a home page to log into to show the authentication working | Co |
| Be able to manipulate data | The ability to delete users from the database | S |
| Economy of mechanism/ease of use | The interface for the end user to be simple and easy to navigate, text or icons will make it as self-explanatory to be able to navigate around | Co |

|  |  |  |
| --- | --- | --- |
| Non-functional features | Description | priority |
| Storage | Have a database with the biometrics stored in | Mo |
| scalability | Be able to handle as many login details as needed | W |
| Security | Make sure the fingerprints are stored securely and not in a raw image | Mo |
| Availability | The systems need to be useable at least 90% of the time | W |
| Back up and recovery | Periodically backup the fingerprints as so they have a fresh recovery point, in case of data error | Co |
| Error handling  Fault tolerance | Appropriate error handling messages for the user | S |
| Visual and/or confirmation of fail/success logging in | Give some feedback as to the state of logging in, e.g. fail try again or success | S |

In this chapter you explain to the reader the specification of the system you intend to build and, just as importantly, **how** you arrived at those requirements.

Depending on your project, you could include subsections covering:

1. Technical description of existing system/s which your project will integrate with and how it will integrate with those systems.
2. System analysis process (how you acquired the system requirements)
3. Functional Requirements
4. Non-Functional Requirements
5. Requirements Prioritisation and/or specification of Minimum Viable Product (MVP)
6. Technology Choices

# System Design

In this chapter you define how the system will be designed, based on the requirements you have collected.

You could consider using:

1. UML
2. ERD
3. Class Hierarchy
4. Composition Diagrams

Note that this chapter should document your initial intended design, before you start coding. Realistically, your designs may change during the implementation process. This is nothing to worry about. You can explain and critically evaluate important changes (not every small low-level change) in the Implementation chapter.

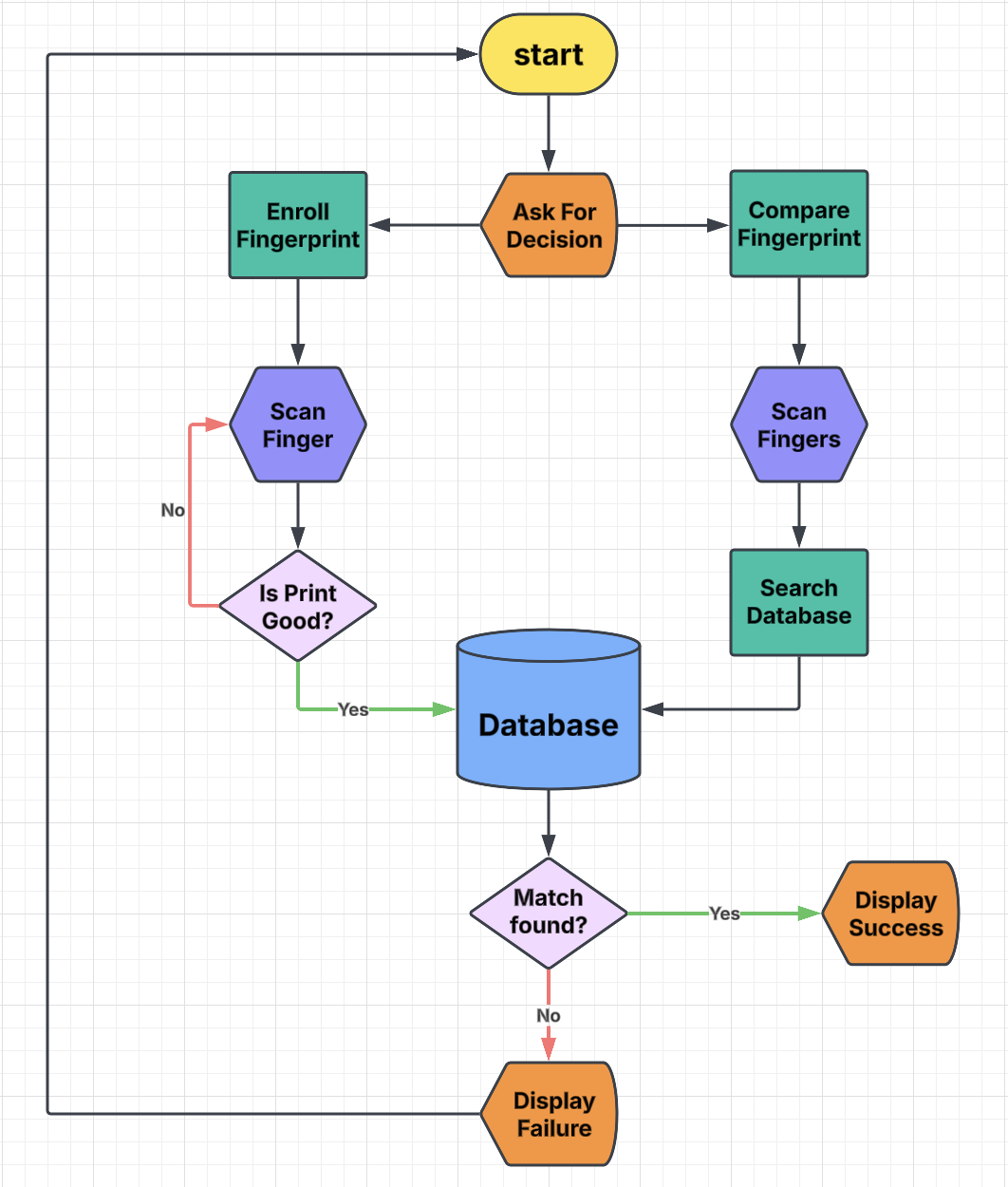


Figure x: Fingerprint system flow

# Implementation + progression (talk implementation of hardware/software)

Work has been undertaken up until now to resource the hardware and decide on the software that would be compatible to work on as well as setting up the development pipeline. Hardware has been set up to work together and work on implementing the scanner and hashing / encryption components with some positive results. During this first development stage, several challenges that required iterative problem-solving and technical adjustments have been encountered. Below an overview of the issues is presented together with the solutions or steps taken to solve these issues.

**Issue 1: Fingerprint Scanner Model Creation.** The initial challenge was the inability of the fingerprint scanner to convert the finger image into a usable model. To resolve this, a solution was devised where two fingerprint scans were combined to generate a single, successful model. This approach overcame the initial hurdle effectively.

**Issue 2: Exporting the Model to Python.** The next obstacle involved exporting the fingerprint model in a format that could be read by Python. This required enabling data transmission via the serial interface. After generating the model, a method was developed to write the data to the serial port, enabling Python to read it successfully.

**Issue 3: Initiating the Fingerprint Scanner from Python.** A further challenge was initiating the fingerprint scanner directly from Python. To achieve this, the Arduino system was configured to respond to a specific command sent via the serial port. Python code was then written to send the command, allowing the Arduino to interpret it as an instruction to start the program. This integration allowed seamless interaction between Python and the scanner.

**Issue 4: Reading Data in Python.** Reading the serial data in Python posed significant difficulties. Various methods were tested to establish a connection with the Arduino and display incoming serial data. Issues with data flow necessitated introducing delays to ensure proper data transmission. A dedicated Python function was created to continuously read the serial data while it was being populated. This approach ensured that the data could be printed and utilized effectively.

**Issue 5: Saving Fingerprint Data.** The fingerprint data generated by the scanner was initially a raw image, which was converted into binary data for processing. While this data could be stored in a database, encryption was required prior to storage. A method was implemented to encrypt the data after capture and before writing it to the serial port. On the Python side, adjustments were made to specify which portion of the data stream to save. The Arduino code was modified to include markers indicating the start and end of relevant data. A Boolean flag controlled the data collection process, ensuring only the desired data was saved to a variable.

**Issue 6: Testing Data Saving.** To validate the saving functionality, a YAML file format was used for testing purposes. YAML, being human-readable, allowed for quick verification of the saved data. Once the functionality was confirmed, the focus shifted to storing the encrypted fingerprint data in a MySQL database.

**Issue 7: Developing a Verification Function.** A verification function was necessary to compare newly captured fingerprints with those stored in the database for authentication. The Arduino code was updated to include an if statement that executed a verification routine when a specific command was received. This routine accessed the database to perform fingerprint comparisons. However, initial implementations faced issues, including failure to return data during enrolment due to serial conflicts.

**Issue 8: Secure Saving.** Initially the data was going to be saved in an encrypted format, later this was changed to using a hash of the fingerprint, as the idea to solve the problem of finding a matching print in the database. The theory behind it was based off normal passwords matching. The print would be hashed and compared with all the hashes to find a match, as they would come out the same. This was an issue however as small differences, such as pressure, on the imaging of a finger would cause a big change in the hash output. To combat these issues, I looked into ways to have an error acceptance level. I researched into this idea and found hammering distancing, this is an algorithm that checks the binary format of two equal length strings, it counts how many bits are different and you can set the limit on these. After implementing, I found it didn’t work, the difference in print data proved too much, so more research showed me \_\_\_\_\_ The data saving format therefore went back to encryption.

**Issue 9: sending data to Arduino.** As a method to try and authenticate users, I planned to use the Arduino built in method that can compare prints. the only issue with this idea, was that the Arduino can only compare with a print on the buffer/hardware database. My initial idea was to send the prints over to the Arduino database. To do this I would need to use the same method as sending them to python, chunking data. While trying to apply the sending back to the Arduino however, the issue of overhead came into play, as the Arduino has a preferred reading speed. This means that on a small scale it would most likely be okay to use but scaling is a huge problem for this method.

Several debugging techniques, such as using print statements in the Arduino code, identified the root cause as buffer overflow during serial communication. To address this, a chunking method was implemented, which divided the data into smaller, manageable pieces for transmission. This adjustment resolved the issue, enabling successful enrolment while maintaining the verification method in the code.

In this chapter you document what actually happened, based on the initial plan and requirements. It should take the reader through the main stages of implementation, focusing on important aspects of the design. Do not try to explain every line of code in this section. It is up to you to decide which are the most important/interesting aspects to discuss. You should critically evaluate any problems/challenges you encountered and the resultant solution or workaround. This is a very good opportunity to demonstrate your skills and ability to carry out critical evaluation. Any changes to the initial design should be explained and justified concisely.

# Testing and Evaluation

## Tests

### Capturing Fingerprint

### Storing Fingerprint

### Verifying Fingerprint

### Deleting Fingerprint

In this chapter you should document the results of the tests you have carried out against the requirements and design, as specified in previous chapters. This may also include results of user testing if appropriate.

Testing may result with large volumes of test results which would not be appropriate to include in the main text and would make the appendices excessively large. If this is the case, it may be worth considering placing large volumes of test data as a separate digital file upload into Brightspace, or include a sample of tests in your appendices if there are too many. However, do not expect assessors to read every page of your tests, they will be more interested in the outcomes of those tests rather than the documentation of vast amounts of individual tests.

# Maintenance and Deployment

This chapter is optional depending on the project. If you do use this chapter, provide an overview of how the system is deployed, and any limiting factors on deployment issues which a user should be aware of. Which other software or libraries must be installed? A full installation guide would be useful. Describe how the system can be patched and upgraded. Are if there are licencing issue to consider?

# Results and Discussion

In this chapter you critically evaluate the overall effectiveness of the initial design. Assessors will be looking for evidence that you can ‘objectively critically evaluate’ your work. This means considering both the positive and negative aspects of your project to demonstrate your problem solving and decision-making skills. Whenever possible, you should support your discussion with citations to demonstrate that you are evaluating your work in the context of your wider field of study.

You should also address how many of the initial requirements were achieved, and why some were not. Think carefully about using phrases such as “***Due to time constraints*** *some requirements were not achieved*”. This leaves yourself open to criticism that you initially over specified the initial design within the available time, or that you suffered from feature creep or that you did not adhere to your proposed plan. Any of these scenarios suggest poor project management. This is why it is important to plan your requirements realistically.

See this library link to help you with Critical Thinking: [Critical Thinking & Writing - Academic Writing - Learning and Teaching at University of Suffolk (uos.ac.uk)](https://libguides.uos.ac.uk/academic-writing/critical-thinking-writing)

# Future Work

Use the limitations of your project, as outlines in the ‘Results and Discussion’ chapter, to identify further improvements to the existing implementation as well as new functionality. This chapter should act as a jumping-off point for other readers (and/or yourself) to continue your work.

# References

[RefWorks & Reference Management - Academic Skills - Learning and Teaching at University of Suffolk (uos.ac.uk)](https://libguides.uos.ac.uk/academicskills/RefWorks)

Elkstrom, M., Lusty, L., Sexton, J,. Sweetnam, J,. Townsend, A,. (2020) *Data Integrity: Identifying and Protecting Assets Against Ransomware And Other Destructive Events*. Available at: https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html (Accessed: 20th November 2024).

Idrus, S. Z. S., Cherrier, E., Rosenburger, C. and Schwartzmann, J. (2013) '*A Review On Authentication Methods*', HAL open science, Australian Journal of basic and Applied science pp 95-107. (Accessed: 13th December 2024)

Kamal, P. (2019) *security of passwords hashing in cloud*. Cloud State University, USA. Journal Of Information Security. Vol.10 No.2

(Accessed 2nd January 2025)

Kurtanovic, Z,. Maalej, W. (2017) *Automatically Classifying Funtional and Non-functional Requirements Using Supervised Machine Learning.* Lisbon, Portugal., Publisher: IEEE, p 1(Accessed: 8th January 2025)

Random Nerd Tutorials(2019) *Guide To Fingerprint Module with Arduino (FPM10A)*  Available at: https://randomnerdtutorials.com/fingerprint-sensor-module-with-arduino/ (Accessed: 13th December 2024).

M.H.Ali, M., Mahale, V and Yannawar, P., A.T, G (2016) *Overview of Fingerprint Recognition System*. Chennai, India: IEEE. **DOI:**[10.1109/ICEEOT.2016.7754900](https://doi.org/10.1109/ICEEOT.2016.7754900) (Accessed 2nd April 2025)

Orandi, S and McCabe, R.M. (2009) *Mobile ID device best practice recommendationvarsion 1.0*. National Institute of Standards and Technology (NIST), NISTSpecial Publication 500–280.

Phillips, J., Martin, A., Wilson, C.L. and Przybocki, M. (2000) *An Introduction to Evaluating Biometric Systems*. Computer. IEEE. Volume: 33, Issue 2. pp. 56-63. DOI: [10.1109/2.820040](https://doi.org/10.1109/2.820040)

(Accessed 1st April 2025)

Saavedra, B.F., Reillo, R.S., Gomez, R.R., Jimenez, J.L. (2016) *small fingerprint scanners used in mobile devices: the impact on biometric performance*. University of Madrid, Spain. IET Biometrics.

(Accessed 4th April 2025)

Shingari, N,. Mago, B. (2024) *The Importance Of Data Encryption in Ensuring the Confidentiality and Security of Financial Records of Medical Health*. Gwalior, India: IEEE.

(Accessed: 3rd January 2025)

Unar, J.A., Seng, W.C. and Abbasi, A. (2014) Pattern Recognition, *A review of biometric technology along with trends and prospects*. Available at: DOI: <https://doi.org/10.1016/j.patcog.2014.01.016>

(Accessed 4th April 2025)

Velasquez, I., Caro, A and Rodriquez, A. (2018) Information and Software Technology. *Authentication Schemes and Methods: A Systematic Literature Review.* Science Direct. Volume: 94. pp 30-37. DOI:<https://doi.org/10.1016/j.infsof.2017.09.012>

(Accessed 4th April 2025)

# Bibliography

A bibliography is optional. A bibliography includes all sources which were consulted in the process of the project but not cited in the main text. This should be presented in the same format as the References.

# Appendix A

Appendices are optional.

If you have any information which is **OPTIONAL** and **NOT ESSENTIAL** for the reader, but you think they may find it interesting, place it in an appendix. The reader will refer to it **IF** they want to. The reader is not expected to read anything in the appendix as this is optional information. In the same sense, do not assume that anything you place in the appendix will be read by the assessor. Assessors are not obliged to read the appendices or consider any of their contents in the marking process. Markers will check the appendices are not being overused, but not necessarily consider their content.

The appendices are not a dumping ground for more ‘stuff’ which you cannot fit within the word limit in the main document. It is wrong to believe that the more ‘stuff’ you cram into the appendices, the higher marks you will receive. Quite the opposite, overuse of the appendices will be penalised. The appendices should not be longer than the report itself.

Use letter identification for each appendix: Appendix A, Appendix B…..

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 2: Test Table 1