|  |  |
| --- | --- |
| m | **Qatar University**  **College of Engineering**  **Department of Computer Science and Engineering** |

Senior Project Report

**<ToDo: Insert Project Title />**

**Project Group Members:**

<ToDo: StudentName1 (StudentId1)

StudentName2 (StudentId2)

StudentName3 (StudentId3) />

**Supervisor**: <**ToDo:** Supervisor Name />

**Co-Supervisor**: <Remove if not applicable/>

**20??**

This project report is submitted to the Department of Computer Science and Engineering of Qatar University in partial fulfillment of the requirements of the Senior Project course.

# Declaration

This report has not been submitted for any other degree at this or any other University. It is solely our work except where cited in the text or the Acknowledgements page. It describes work carried out by us for the senior project. We are aware of the university policy on plagiarism and the associated penalties and we declare that this report is the product of our own work.

< **ToDo:** For each student add the signature and the date of signing the declaration />

Student: Date:

Signature:

Student: Date:

Signature:

Student: Date:

Signature:

Table of Contents

[Declaration ii](#_Toc127951596)

[Abstract iii](#_Toc127951597)

[Acknowledgment iv](#_Toc127951598)

[List of Figures vii](#_Toc127951599)

[List of tables viii](#_Toc127951600)

[1. Introduction and Motivation 9](#_Toc127951601)

[1.1. Problem statement 9](#_Toc127951602)

[1.2. Project objectives 9](#_Toc127951603)

[1.3. Expected benefits and impacts on various contexts 9](#_Toc127951604)

[1.4. Market Research and Business Viability 10](#_Toc127951605)

[2. Background and related work 10](#_Toc127951606)

[2.1. Background 10](#_Toc127951607)

[2.2. Related work 11](#_Toc127951608)

[3. Requirements analysis 12](#_Toc127951609)

[3.1. Software development process 12](#_Toc127951610)

[3.1.1. Applying the software development process 12](#_Toc127951611)

[3.2. Functional requirements 12](#_Toc127951612)

[3.3. Non-functional requirements 13](#_Toc127951613)

[3.4. Assumptions 14](#_Toc127951614)

[3.5. Ethics 14](#_Toc127951615)

[4. Project Plan 15](#_Toc127951616)

[4.1. Project milestones 15](#_Toc127951617)

[4.2. Project timeline 15](#_Toc127951618)

[4.3. Anticipated risks 15](#_Toc127951619)

[5. Solution Design 16](#_Toc127951620)

[5.1. High-level design 16](#_Toc127951621)

[5.1.1. Alternative solutions and tradeoffs 16](#_Toc127951622)

[5.1.2. Selected solution overview 16](#_Toc127951623)

[5.1.3. High level architecture 17](#_Toc127951624)

[5.2. Structural model 17](#_Toc127951625)

[5.3. Behavioral model 17](#_Toc127951626)

[5.4. Database design 18](#_Toc127951627)

[5.5. User interface design 18](#_Toc127951628)

[5.6. Design patterns 18](#_Toc127951629)

[6. Implementation 19](#_Toc127951630)

[6.1. Hardware/software used 19](#_Toc127951631)

[6.2. Challenging issues and solutions 19](#_Toc127951632)

[7. Testing and evaluation 20](#_Toc127951633)

[7.1. Functional testing 20](#_Toc127951634)

[7.2. Non-functional testing 20](#_Toc127951635)

[8. Conclusion 21](#_Toc127951636)

[9. Future work 22](#_Toc127951637)

[10. Student reflections 23](#_Toc127951638)

[References 24](#_Toc127951639)

[Appendix A – Use cases specification 25](#_Toc127951640)

[Appendix B – Test cases specification 26](#_Toc127951641)

[Other Appendices 27](#_Toc127951642)

## Market Research and Business Viability

< **ToDo:**

* Conduct market research to address the following:
* Describe the market need and the market size.
* Identify the target customers and their demographic.
* Describe the competing products and how does yours differ from that offered by competitors? Highlight the novel features of your product and the benefits it offers.
* Develop a business plan including your business model, pricing, marketing strategy to bring your product to market and make it competitive.

/>

Our application targets the main public including students, employees, business men…etc, but it can be customized and improved/extended for specific business fields/goals (for eg. For a specific company that requires extra features, or governmental security…etc). as explained in section 1.1 password cracking is becoming more and more frequent //make sure to state that in 1.1// for that it serves the main public. A survey has been conducted on 227 respondents (146 males, 81 females), from different age groups, sectors and occupations as shown in figures ….

Forms response chart. Question title: الفئة العمرية
. Number of responses: 175 responses.

Forms response chart. Question title: Age group
. Number of responses: 52 responses.

Forms response chart. Question title: Field of Study
. Number of responses: 51 responses.

Forms response chart. Question title: مجال التخصص (عمل أو دراسة)
. Number of responses: 175 responses.

Forms response chart. Question title: العمل
. Number of responses: 175 responses.Forms response chart. Question title: Occupation
. Number of responses: 52 responses.

The survey analysis consisted of three main points:

1. Survey sample scope analysis

Based on all of the above the sample was categorized into 8 main groups based on common & significant characteristics (job, age..etc) that will help to get better understanding and analysis of the answers

Target groups:

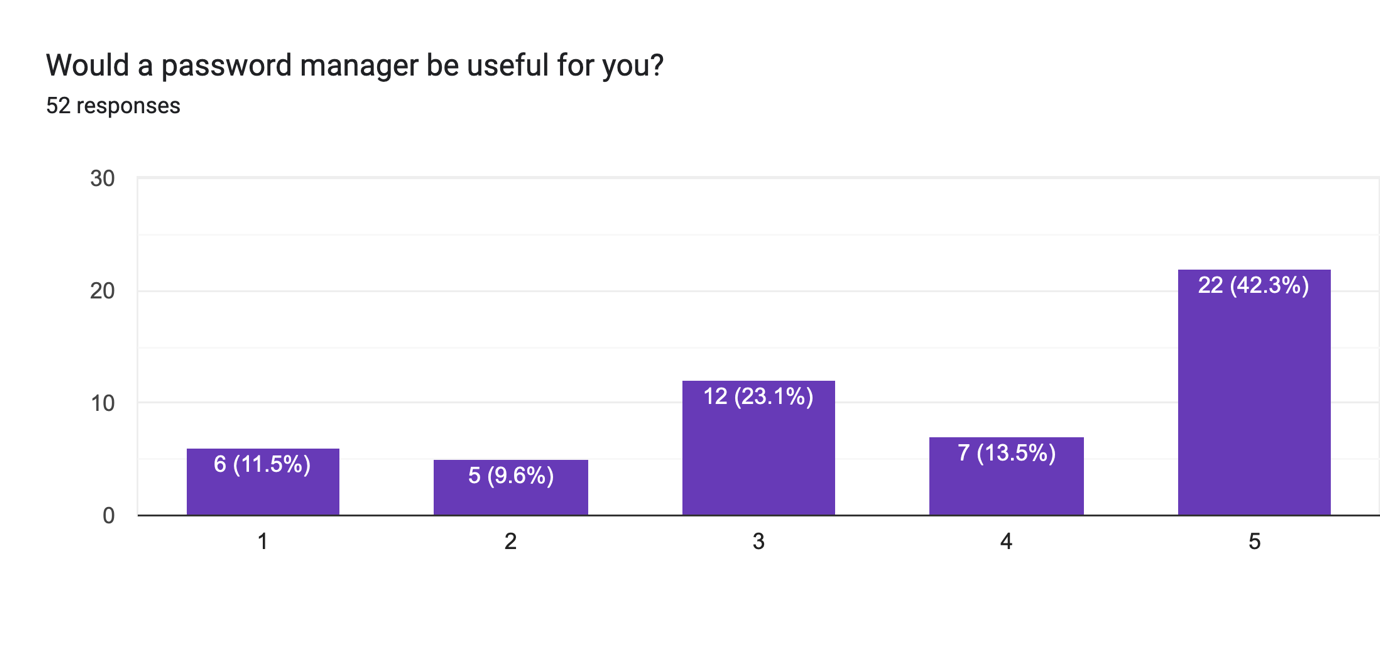
1. Engineering male student (18-25 years): 64
2. Non-engineering male student: 29
3. Engineering female student : 22
4. Non-engineering female student: 20
5. Female employee (+20years) : 27 (11 are in education ; 22 are above 30 years)
6. Male employee (+20years) : 38 (17 in education, 10 in engineering)
7. Housewife: 6
8. Male & female (-18years) : 12

Targets represent 97.3% of total data set

//The analysis considers the overall top 2 answers as well as the top answer in each category.

1. Need for the application (based on the sample scope)

First, the direct question was asked in the survey: ”Would a password manager be useful for you?”. 42% of respondents considered that a password manager would be very useful for them.

Forms response chart. Question title: إلى أيّ درجة سيكون برنامج إدارة كلمات المرور مفيدا لك؟
. Number of responses: 175 responses.

A number of questions were then addressed to assess the extent to which the application is needed based on two aspects:

1. Security behavior

It covered four main points which consists the main services that a password manager tries to ease: location/way of saving the passwords, frequency of forgetting the passwords, frequency of reusing a password, and if they have been hacked before.

31.8% answered that they just memorize their passwords, while 25.6% save it in a file in phone or computer, only 14.4% uses a password manager. 38.7% mentioned that sometimes they forget their passwords (2 on a scale of 5). 36% of the respondents reuse the same password for 1 to 3 accounts, and 31% for 4 to 10 accounts. Most of the respondents had never got their passwords leaked before, only a few (12%) mentioned that have been a victim of a cyber-attack 1 to 3 times. It is good to mention that 52.4% of respondents did not hear about password managers before, which may explain the infrequent use of it.

It can be concluded that people still rely on traditional behavior to save and use their passwords, which proves that security behavior should be implemented in more efficient way……..

(still to add the significant conclusion from the analysis of each category)

1. Security knowledge

As the application is meant to be for the general public, it should be assumed that the user does not have any prior security knowledge. Here, we wanted to know if people are aware about their password strength or not. It has been done by asking the direct question: “How strong do you think your passwords are?”. And then, show them the following figure that shows the actual password strength, and ask the question again to spot/see/assess the gap between what they thought and the actual strength of their password

(for each category)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Password strength self-evaluation 1 | Color in figure | Password strength self- evaluation 2 | Matching | Gap |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |



Ref[]

(better to mention which group had biggest mistake) It might be our mistake since we did not explain the picture, but overall it proves that not only people assess their password strength wrongly (u gave the % before of the “gap” + the actual matching/almostMatching values) but also don’t understand difficult things > low security knowledge.

* Shouldn’t assume that the user understands > when doing the implementation (especially add/update password) we should take that into consideration, for eg. Put guidelines, easy activity flows, simple GUI…etc

//draft

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | location | forgetting | reusing | Hacked before |
| Top 1 | Memorization (…%) | 2/5 | 1-3 times | never |
| Top 2 | On a file in phone or pc | 3/5 | 4-10 times | Idk & 1-3 times |
| Engineering male student | File in phone or pc |  |  |  |
| Non-engineering male student |  |  |  |  |
| Engineering female student |  |  |  |  |
| Non-engineering female student |  |  |  |  |
| Female employee (+20years) |  |  |  |  |
| Male employee (+20years) |  |  |  |  |
| Housewife |  |  |  |  |
| Male & female (-18years) |  |  |  |  |

1. business consideration & application features

Then, we wanted to know the main features that users would like to have in a password manager. Survey answers show that the most important accounts that people want to protect are: bank account (more than 60%), email account (around 50%), and social media (around 50%). Concerning the pricing, 70 % are not willing to pay for such service, and only 25% are willing to pay for the time (not subscription) which represents a business challenge that should be solved either by having a strong marketing strategy to convince people to pay for it, or by finding an income source, not from the customers directly.

61% trust using a password manager. The main reasons for the rest not to trust are:

* Main concern: Privacy untrust in third-parties (especially non-open source)
* Fear of the app getting hacked, therefore passwords leaked, especially that it will be a target for hackers
* Not knowing about the application

Hopefully, these issues are addressed in prior in our business plan:

* Users can trust the application since it is offline, on their own devices. If passwords would have been saved online, then privacy would have been an issue.
* The decentralization of databases (each user has his own local database) would make it non convenient for hackers to target our users. However, the hackers could use some vulnerabilities in the application to target multiple users. Therefore, this technical challenge should be taken into consideration by the implementation and security team.
* We need to include an informative process in the marketing plan to introduce password managers since a lot of people do not know it.

Regarding the features, almost all suggested features (listed below) were equally demanded by respondents. Generation of strong password, password recovery, and auto-fill features had a small higher demand than other features.

Regarding portability, the big majority preferred the app to be in smartphone, and less preferred it to be on desktop. For now, we aim to make it a desktop app, and in the future work we aspire to make it available as a mobile app.

Finally, we received suggestions from respondents, the most significant ones were:

* To use MFA mechanisms for authentication
* Having multiple fail-safes in case of losing the ability to access primary account or device. other than "forget password" would be a great addition
* Make it open-source

Business plan:

Model:

Pricing:

Marketing: