Feasibility Report

for

Cryptographically - Secure Password Manager

Version 1.0

Prepared by

Anushka Singh | 2021IMG-014
Avijeet Jain | 2021IMG-018
Yuvraj Kumar | 2021IMG-066

ABV-Indian Institute of Information Technology & Management, Gwalior

20th March 2022

Submitted in partial fulfillment
Of the requirements of
IMIT-2202 Software Engineering Lab

TABLE OF CONTENTS

1. Introduction

1.1 Overview of the Project

Our Project PassMan - A Cryptographically Secured Password Manager project aims to develop a secure and user-friendly password manager application that protects user data with strong encryption and multi-factor authentication. The application will enable users to store, manage, and retrieve passwords for multiple online accounts in a secure and reliable manner.

The project will involve designing and developing a password manager application with a user-friendly interface that makes it easy for users to manage their passwords, generate secure passwords, and view their password strength and expiration dates. The application will also include cryptographic functions, such as encryption algorithms, key management, and secure random number generation, to protect user data.

In addition, the password manager application will have a database to store user data and passwords securely. The database will be able to handle multiple users, and passwords will be encrypted and hashed for added security. The application will also be scalable to handle multiple users and passwords without compromising security or performance.

1.2 Objectives of the Project

The objectives of the Cryptographically Secured Password Manager project are as follows:

- Develop a secure password manager: The primary objective of the project is to develop a secure password manager application that protects user data with strong encryption and multi-factor authentication. The application should be able to store, manage, and retrieve passwords for multiple online accounts in a secure and reliable manner.

- Create a user-friendly interface: The password manager application should have a user-friendly interface that makes it easy for users to manage their passwords, generate secure passwords, and view their password strength and expiration dates. The interface should be intuitive and easy to use, even for users with limited technical knowledge.

- Ensure compliance with data protection laws: The password manager application should comply with relevant data protection and privacy laws, such as GDPR and HIPAA. This would include providing users with the option to delete their data and ensuring that user data is stored and transmitted securely.

- Integrate with different web browsers and operating systems: The password manager application should integrate seamlessly with different web browsers and operating systems to provide a seamless experience for users. This would include Chrome, Firefox, Safari, and Windows, among others.

- Provide testing and quality assurance: The project should include testing and quality assurance to ensure that the password manager application is secure, reliable, and user-friendly. This would include functional testing, security testing, and performance testing.

- Ensure scalability: The password manager application should be scalable to handle multiple users and passwords without compromising security or performance. The application should be able to handle the storage and retrieval of large amounts of data in a secure and efficient manner.

1.3 The Need for the Project

The need for the Cryptographically Secured Password Manager project arises from the increasing importance of password security in today's digital age. With the growing number of online accounts that people use on a daily basis, the need for strong and unique passwords for each account is crucial to prevent unauthorized access and data breaches.

However, it can be difficult for individuals to manage multiple strong passwords without using a password manager. Password managers provide a secure and user-friendly method of storing, managing, and retrieving passwords for multiple online accounts. They also provide automatic password generation, ensuring that passwords are unique and strong.

In addition, the increasing number of data breaches and cyber attacks has made password security even more critical. Cybercriminals can use stolen passwords to access sensitive information, steal identities, and commit fraud. A secure password manager can help prevent these types of attacks by ensuring that passwords are stored and transmitted securely using strong encryption and multi-factor authentication.

Therefore, the need for a Cryptographically Secured Password Manager project is clear. It would provide a secure and reliable method of managing passwords, ensuring that users can protect their online accounts and sensitive information from unauthorized access and data breaches.

1.4 Overview of Existing Systems and Technologies

Strong passwords are the linchpin of any company's cyber security strategy. IT teams around the world have put in place policies surrounding password security and especially password strength.

With numerous high-profile social media data breaches over the years, password reuse has become a significant issue. Many people use the same password for their personal and work accounts, so another company's poor security can quickly become your problem.

Even with strong passwords, your organization can still be at risk of breaches because of passwords being reused across accounts and websites. In 2019, Microsoft compared their password databases with breached credential databases and found 44 million accounts that were reusing passwords. Microsoft then forced a password reset on all these users.

1.5 Scope of the Project

The scope of the Cryptographically Secured Password Manager project would include the development of a software application that allows users to securely store, manage, and retrieve passwords for multiple online accounts. The application would need to include strong encryption and multi-factor authentication to ensure the security of user data. The scope would also include the development of a user-friendly interface for managing passwords and generating secure passwords.

The project would require the development of a database to store user data and passwords securely, as well as the implementation of necessary cryptographic functions to protect the data. The password manager would need to integrate with different web browsers and operating systems to provide a seamless experience for users.

In addition to the technical development of the password manager, the scope would also include testing and quality assurance to ensure the security and functionality of the application. The project would also require compliance with relevant data protection and privacy laws, such as GDPR and HIPAA.

Overall, the scope of the project would be to develop a robust and secure password manager application that provides users with a user-friendly and reliable method of managing their passwords and ensuring the security of their online accounts.

1.6 Deliverables.

The following are the deliverables of the Cryptographically Secured Password Manager project:

- Software Application: The primary deliverable of the project would be the software application itself. This would include a password manager application that is secure, reliable, and user-friendly. The application should be able to store, manage, and retrieve passwords for multiple online accounts using strong encryption and multi-factor authentication.

- User Interface Design: The user interface design for the password manager application should be intuitive and easy to use. The design should allow users to manage their passwords, generate secure passwords, and view their password strength and expiration dates.

- Cryptographic Functions: The password manager application should include the necessary cryptographic functions to protect user data. This would include encryption algorithms, key management, and secure random number generation.

- Database Management: The application should include a database to store user data and passwords securely. The database should be able to handle multiple users, and passwords should be encrypted and hashed for added security.

- Integration: The password manager application should be able to integrate with different web browsers and operating systems, such as Chrome, Firefox, Safari, and Windows, to provide a seamless experience for users.

- Testing and Quality Assurance: The project should include testing and quality assurance to ensure that the password manager application is secure, reliable, and user-friendly. This would include functional testing, security testing, and performance testing.

- Compliance: The password manager application should comply with relevant data protection and privacy laws, such as GDPR and HIPAA. This would include providing users with the option to delete their data, as well as ensuring that user data is stored and transmitted securely.

Overall, the deliverables of the Cryptographically Secured Password Manager project would include a robust and secure password manager application that provides users with a user-friendly and reliable method of managing their passwords and ensuring the security of their online accounts.

2. Feasibility Study

The purpose of this feasibility report is to assess the viability and potential success of a Cryptographically Secured Password Manager. The password manager would provide a secure and user-friendly method of storing, managing, and retrieving passwords for multiple online accounts. The key features of the password manager would include strong encryption, multi-factor authentication, and automatic password generation.

2.1 Financial Feasibility

The development of a Cryptographically Secured Password Manager would require a significant initial investment in software development and infrastructure. However, the potential for revenue is significant. The most common business model for password managers is a subscription-based model, where users pay a monthly or annual fee for access to the password manager. Additionally, the password manager could be offered as part of a larger suite of security products, such as antivirus software or firewalls, which could increase revenue potential.

The system will follow the freeware software standards. No cost will be charged from the potential customers. Bug fixes and maintaining tasks will have an associated cost.
At the initial stage the potential market space will be the local universities and higher educational institutes.

Beside the associated cost, there will be many benefits for the customers. Especially the extra effort that is associated with paper making and marking will be significantly reduced while the effort to create descriptive statistical reports will be eliminated, since reports generation is fully automated.

From these it’s clear that the project PassMan is financially feasible.

2.2 Technical Feasibility

From a technical perspective, the development of a Cryptographically Secured Password Manager is feasible. There are many existing password managers that use encryption and other security measures to protect user data. Open-source libraries and frameworks, such as OpenSSL and cryptography.io, can be used to implement the necessary cryptographic functions. Additionally, the user interface and database functionality can be developed using popular web development frameworks, such as React, Angular, or Vue.js.

Each of the technologies are freely available and the technical skills required are manageable. Time limitations of the product development and the ease of implementing using these technologies are synchronized.
Initially the web site will be hosted in a free web hosting space, but for later implementations it will be hosted in a paid web hosting space with a sufficient bandwidth. Bandwidth required in this application is very low, since it doesn’t incorporate any multimedia aspect.

From these it’s clear that the project PassMan is technically feasible.

2.3 Resource and Time Feasibility

Resources that are required for the PassMan project includes:

- Programming device (Laptop)
- Hosting space (freely available)
- Programming tools (freely available)
- Programming individuals

So it’s clear that the project OES has the required resource feasibility.

2.4 Risk Feasibility

There are several potential risks associated with the Cryptographically Secured Password Manager project, which should be considered during the feasibility analysis. Some of the key risks are as follows:

- Security risks: The primary risk associated with a password manager application is security. The application will store sensitive information, including passwords, and must be designed with robust security features to prevent unauthorized access and data breaches. The application must be designed with strong encryption algorithms, secure key management, and multi-factor authentication to ensure the security of user data.

- Integration risks: The password manager application must integrate seamlessly with different web browsers and operating systems to provide a seamless experience for users. This can be challenging, as different systems have different security features and compatibility requirements. Ensuring compatibility with various platforms and browsers may require additional development efforts and testing.

- User adoption risks: User adoption is another potential risk associated with the password manager application. Some users may be hesitant to use a password manager, preferring to manage their passwords manually. Educating users on the benefits of using a password manager, and providing clear and intuitive instructions on how to use the application, can help mitigate this risk.

- Regulatory risks: The password manager application must comply with relevant data protection and privacy laws, such as GDPR and HIPAA. Failure to comply with these regulations could result in legal and financial penalties.

- Performance risks: The application must be designed to handle large amounts of data and multiple users without compromising security or performance. Ensuring that the application performs well and is scalable may require additional development efforts and testing.

Overall, the risks associated with the Cryptographically Secured Password Manager project can be mitigated through careful planning, testing, and adherence to best practices in security and software development. A thorough risk assessment and mitigation plan should be developed and implemented throughout the project to ensure that potential risks are identified and addressed in a timely and effective manner.

2.5 Social/Legal Feasibility

There are several legal and ethical considerations to take into account when developing a password manager. The primary ethical consideration is the need to protect user data and privacy. The password manager must use strong encryption and security measures to prevent data breaches. Additionally, the password manager must comply with relevant data protection and privacy laws, such as GDPR in the European Union, CCPA in California, and HIPAA in the US healthcare sector.

3. Considerations

Performance

The performance of the Cryptographically Secured Password Manager project can be measured in terms of several key metrics, including speed, scalability, and reliability.

Speed

The speed of the password manager application will be an important consideration for users. The application should be designed to provide fast and responsive performance, even when handling large amounts of data. This can be achieved through optimization of database queries, efficient encryption algorithms, and use of caching and other performance-enhancing techniques.

Scalability

The password manager application should be able to handle multiple users and large volumes of data without compromising performance or security. This requires careful design and architecture, with attention to scalability issues such as database design, load balancing, and resource management.

Reliability

The password manager application must be reliable and available to users at all times. This can be achieved through robust testing and quality assurance processes, including load testing, functional testing, and performance testing. The application must also have appropriate backup and recovery mechanisms in place to ensure that user data is protected in the event of a system failure or other issue.

User authentication

Users will have to authenticate using the username and passwords. Depending on the access level each user will gain functionality of the system. Passwords can be changed by the user.

Login details

Each user’s login time and logout time will be recorded in the system, to make the tractability process easy in case of a faulty action.

Usability and ease of use

Users will be provided with a complete user manual as a pdf. The interfaces are designed to make it easy for any potential user to get familiar with the system within one hour. No additional training is required to use the system.

Availability

System will be available throughout the 24 hours. Mean time to failure and mean time to repair will be decided to increase the availability. With a paid hosting space, the availability can be guaranteed to a great precision.

Maintainability

PassMan is designed using the best practices of RUP and OOP. Since every single segment in the system is very well structured, the system is highly maintainable. 4+1 view model will be used as the main architectural pattern in this system. Hence the separation of each task is improved, hence maintainability improved.

4. Conclusion

In conclusion, the development of a Cryptographically Secured Password Manager is technically feasible, with existing libraries and frameworks available to implement necessary cryptographic functions. The market potential for a password manager is high, given the growing need for strong password security. The financial potential for a password manager is also significant, with the most common business model being subscription-based. The primary ethical consideration is protecting user data and privacy, which requires strong encryption and compliance with relevant data protection and privacy laws.

5. References

IEEE Std 830-1998 IEEE Recommended Practice for Software Requirements Specifications. IEEE Computer Society, 1998.