Individual Project (CS3IP16)

Department of Computer Science
University of Reading

Project Initiation Document

PID Sign-Off

Student No.	**30021310**
Student Name	**Ajuyah Akatomisan Michaelangelo**
Email	**wt021310@student.reading.ac.uk**
Degree programme (BSc CS/BSc CSwIY)	**BSc CS**
Supervisor Name *(Consultation with supervisor is mandatory)*	**Martin Lester**
	Supervisor to sign PID form on Bb (grade centre)
Date	**22 Jan 2024**

SECTION 1 – General Information

Project Identification

1.1	**Project Title**
	FortiVault: Architecting the Future of Digital Security through Password Management
1.2	**Please describe the project with key-phrases (max 5)**
	AES-256, Password, Authorization, Cybersecurity, User-friendly
1.3	**E-logbook maintenance agreed with supervisor** *Use Google doc, OneDrive, or any mobile App whereby you will be able to generate a PDF copy*
	Google Doc
1.4	**GitLab link for maintain source code and research data** *Any change in GitLab link and Source code repository MUST be explicitly mention in final report*
	https://csgitlab.reading.ac.uk/wt021310/final-year-project

SECTION 2 – Project Description

2.1	**Summarise the project's background in terms of research field /application domain (max 100 words).**
	The project aims to address the critical issue of password security in the digital era. It presents an advanced password manager, FortiVault, designed using cutting-edge web technologies like Next.js 14, Prisma, PostgreSQL, Supabase, OAuth 2.0 with Google, and NextAuth for secure authentication. The project highlights the increasing importance of secure and user-friendly password management systems due to the rising threats of data breaches and unauthorized access. FortiVault stands as a testament to combining modern web development and cybersecurity principles to enhance individual password security and contribute to the broader discourse on personal data protection in the digital landscape.
2.2	**Summarise the project aims, objectives and outputs (max 250 words).** These aims, objectives, and outputs should appear as the tasks, milestones and deliverables in your project plan (fill out Section 3).
	The project, FortiVault, is designed to bolster digital security through an advanced password management system, addressing the escalating challenge of cybersecurity in the digital age. Aiming to mitigate vulnerabilities in existing password management solutions, FortiVault integrates cutting-edge web technologies—such as Next.js 14, Prisma, PostgreSQL, Supabase, OAuth 2.0 with Google, and NextAuth for authentication—to construct a secure, user-friendly platform for managing sensitive user passwords. Objectives of the project include: 1. Analysing weaknesses in conventional password management systems to enhance security. 2. Employing modern web technologies for developing FortiVault, ensuring a blend of robust security measures and user-friendly experience. 3. Evaluating FortiVault's effectiveness against common cyber threats through comprehensive testing. 4. Enhancing user experience without compromising security, facilitating broader adoption of secure password management practices. The outputs of the project encompass the development of FortiVault, which showcases secure architecture, seamless user experience, and advanced authentication mechanisms. It proposes a practical solution for individual password security, contributing significantly to the discourse on personal data protection. By addressing both technical and user-experience aspects, FortiVault sets a new benchmark in password management, offering a sophisticated tool that aligns with the current needs of digital security.

2.3	**Initial project specification – roughly indicate key features and functions of your finished program/application. Indicate possible method, data source, technology etc. (max 400 words)** (Sensible and relevant Charts, Table, and Figures can be used)

FortiVault is a state-of-the-art password management application designed to address the contemporary challenges of digital security and user experience. It stands out for its integration of advanced web technologies and encryption standards, offering a comprehensive solution for secure password storage and management. Key features and functions of FortiVault include:

1. **Advanced Encryption**: Utilizing AES-256 encryption, FortiVault ensures that all stored passwords are securely encrypted, providing a robust defence against potential cyber threats and unauthorized access. This encryption standard is known for its strength and is widely used in securing sensitive data.

2. **User Authentication**: FortiVault employs NextAuth for seamless and secure user authentication. This includes support for OAuth 2.0 with Google, allowing users to sign in using their Google accounts, thus streamlining the login process while maintaining high security standards.

3. **Intuitive User Interface**: The application is designed with a user-friendly interface, ensuring ease of navigation and functionality. Users can effortlessly manage their passwords, with features such as adding, retrieving, and updating passwords facilitated through a clear and accessible layout.

4. **Password Generation**: FortiVault includes a password generation feature that enables users to create strong, unique passwords. This function helps in promoting better security practices by discouraging the reuse of passwords across multiple sites.

5. **Cross-Platform Accessibility**: Built using Next.js and responsive design principles, FortiVault is accessible across various devices and platforms, allowing users to manage their passwords anytime, anywhere, with consistent user experience.

6. **Secure Data Storage**: Leveraging Prisma and Supabase for backend services, FortiVault offers secure and efficient data storage solutions. This includes real-time database management and secure data synchronization across devices.

7. **Email Verification and Password Recovery**: The application incorporates email verification for new users and a secure password recovery mechanism for those who forget their login details. This ensures that user accounts are verified and that users can recover access to their accounts securely.

8. **Compliance with Security Standards**: FortiVault is designed with a focus on compliance with current security standards, ensuring that the application is equipped to protect user data effectively against evolving cyber threats.

9. **Customizable Security Settings**: Users have the option to customize their security settings within the application, allowing for a personalized security experience that caters to individual needs and preferences.

10. **Community Feedback and Continuous Improvement**: FortiVault is developed with an emphasis on user feedback, facilitating continuous improvement and updates to the application based on user experiences and suggestions.

In summary, FortiVault encapsulates a blend of advanced encryption, user-friendly design, secure authentication, and cross-platform accessibility, making it a comprehensive solution for managing passwords securely and efficiently in the digital age.

2.4	**Describe the social, legal and ethical issues that apply to your project. Does your project require ethical approval? (If your project requires a questionnaire/interview for conducting research and/or collecting data, you will need to apply for an ethical approval)**
2.5	**Identify the items you may need to purchase for your project. A cost upto £200 can be applied (include VAT and shipping if known). You need to have consent of your supervisor. Your request will be assessed by the department.**
2.6	**State whether you need access to specific resources within the department or the University e.g. special devices and workshop**

SECTION 3 - Project Plan

Please provide your project plan.

Below is an example project plan, you can use any tool or software to generate yours.

Project stage [this is only indicative – write your own stages]	**START DATE: 22/01/2024.** **Project Weeks**											
	1	2	3	4	5	6	7	8	9	10	11	12
1 Background Research												
1.1. Encryption												
1.2 Technologies												
2 Analysis/Design												
Analysis of Existing Systems												
Requirement Specification												
3 Develop prototype												
3.1 Programming												
3.2 Debugging												
4 Testing/evaluation/validation												
4.1 System Testing												
4.2 Beta Testing												
5 Documentation												