

PROJECT PROPOSAL

Information Security



BS(CS)-3B

AIR UNIVERSITY ISLAMABAD

Group Members

| Name | Registration-ID |
|---------------|-----------------|
| Afia Aziz | 231561 |
| Zumer Dhillun | 231597 |
| Zoya Azad | 231579 |
| Duaa Dara | 232481 |

Submitted to: Miss Waseeqa Ghazanfer

Project Proposal: Data Hashing Tool

1. Group Information:

Role of each group member:

| Name | Registration ID | Role |
|---------------|-----------------|--|
| Zoya Azad | 231579 | Front-End Code of the first two webpages and documentation of the project. |
| Zumer Dhillun | 231597 | Backend Code of all webpages. |
| Afia Aziz | 231561 | Front-End Code of the 3rd, 4th, and 5th webpages. |
| Duaa Dara | 232481 | Front-End Code of the 6th and 7th webpages. |

2. Project Overview: The proposed project, titled "Data Hashing Tool," is an innovative web-based application aimed at providing a comprehensive suite of hashing-related functionalities to enhance information security. By integrating state-of-the-art hashing algorithms and user-friendly interfaces, this tool is designed to educate users on the importance of hashing, offer practical implementations of security measures, and ensure secure data handling.

The project leverages HTML and CSS for the frontend and Python Flask for the backend, ensuring a seamless and responsive user experience.

Importance for Information Security

Hashing is a cornerstone of secure data management, but many individuals and organizations lack tools to effectively understand and implement hashing techniques. This project bridges this gap by providing an **educational and practical tool**.

3. Objectives

1. To create a user-friendly tool for generating and comparing hashes using widely recognized algorithms such as **MD5, SHA-1, SHA-256, and SHA-512**.
 2. To enhance user understanding of hashing algorithms by providing a **comparison feature** that evaluates their security levels.
 3. To promote secure password practices by offering **password strength evaluations** and the option to create **salted hashes**.
 4. To deliver an aesthetically appealing and functional web interface with distinct pages for each functionality.
-

4. Benefits of the Project:

1. **Enhanced Security Awareness:** The tool provides practical insights into secure data handling, fostering a deeper understanding of cryptographic hashing among users.
 2. **Educational Value:** The algorithm comparison feature enables users to learn about the strengths and weaknesses of different hashing methods.
 3. **Customizability:** The inclusion of salted hash generation offers users advanced security options for safeguarding sensitive information.
 4. **Comprehensive Functionality:** Combining multiple features such as hash generation, hash comparison, password evaluation, and algorithm comparison in one tool increases convenience and usability.
 5. **Visual Appeal:** A professional and modern design ensures an intuitive user experience.
 6. **Realistic Implementation:** The splash screen with a logo and a navigation bar simulates professional tools, enhancing the project's realism and usability.
-

5. Scope of the Project

In-Scope:

- Implementing hashing algorithms (**MD5, SHA-1, SHA-256, SHA-512**).
- Providing a **hash generation and comparison** feature.
- **Salted hash generation** for advanced security.

- **Password strength evaluation** and improvement suggestions.
- Educational comparisons of hashing algorithms.

Out-of-Scope:

- Advanced cryptography implementations beyond hashing algorithms.
 - Physical security measures.
 - Integration with external APIs or services for authentication.
-

6. Why This Project Is Unique:

1. **Integration of Multiple Functionalities:** Unlike typical hashing tools that focus on a single task, this project combines multiple hashing-related functions, making it an all-in-one solution.
 2. **Educational Focus:** The tool is not just functional but also educational, offering algorithm comparisons and password strength analysis.
 3. **Custom Salted Hashing:** By allowing users to generate salted hashes, the tool emphasizes advanced security techniques.
 4. **User Experience:** The inclusion of a loading splash screen and aesthetically pleasing webpages ensures a polished and professional look.
-

7. Tools and Technologies

Tools and Technologies Used:

- **Frontend:**
 - HTML



- CSS



- **Backend:**
 - Python Flask



- **Libraries:**
 - hashlib: For hashing functions.
 - re: For regex-based password validation.
- **Design Elements:**
 - Custom logo and splash screen for branding.

D A T A H A S H I N G T O O L

Why We Chose This Topic: In the current digital age, information security is a growing concern, with hashing being a cornerstone of secure data management. However, many individuals and even organizations lack adequate tools to understand or implement these techniques effectively. This project aims to bridge this gap by providing a practical, educational, and user-friendly solution. Additionally, the project aligns with our academic curriculum, enabling us to apply theoretical knowledge to a real-world problem.

8. Functionalities:

1. **Hash Generation:**
 - Input: Text or files.
 - Algorithms: MD5, SHA-1, SHA-256, and SHA-512.
 - Output: Hash value.
2. **Hash Comparison:**
 - Input: Two hash values.

- Output: Verification of whether the hashes match.
 - 3. **Algorithm Comparison:**
 - Input: Two selected hashing algorithms.
 - Output: Security level comparison.
 - 4. **Salted Hash Generation:**
 - Input: Text or files and a custom salt.
 - Output: Salted hash value.
 - 5. **Password Strength Checker:**
 - Input: User-provided password.
 - Output: Password strength evaluation and improvement suggestions.
-

9. Methodology

The project will follow a structured approach to ensure timely and efficient development:

1. **Research Phase:**
 - Understand different hashing algorithms and their applications.
 - Design the tool's architecture.
 2. **Implementation Phase:**
 - Develop the frontend using **HTML and CSS**.
 - Build backend functionality with **Python Flask** for generating hashes, comparing algorithms, and evaluating passwords.
 - Integrate all features into a cohesive system.
 3. **Testing Phase:**
 - Validate functionalities, including hash generation, comparison, and password strength checks.
 - Fix any bugs and ensure accuracy.
 4. **Documentation Phase:**
 - Prepare a detailed project report.
 - Develop a user manual for the tool.
-

10. Deliverables

At the end of the project, we will deliver:

- **A fully functional web-based hashing tool.**

- A **project report** detailing the tool's functionality, implementation, and use cases.
 - **Tool configuration files or code** for review and evaluation.
 - A **presentation and demonstration** of the project outcomes.
-

11. Expected Outcomes

1. A secure and efficient tool for generating, comparing, and analyzing hash values.
 2. A deeper understanding of cryptographic hashing for users.
 3. Practical insights into password security through the password strength evaluator.
 4. A polished, professional user interface with real-world applications.
-

12. References

1. Documentation for hashlib library: <https://docs.python.org/3/library/hashlib.html>
 2. Flask official documentation: <https://flask.palletsprojects.com>
 3. Articles on hashing algorithms and their applications in cybersecurity.
 4. Tutorials and resources for frontend development using **HTML and CSS**.
-

13. Appendix

Diagrams, Charts, and Supporting Information:

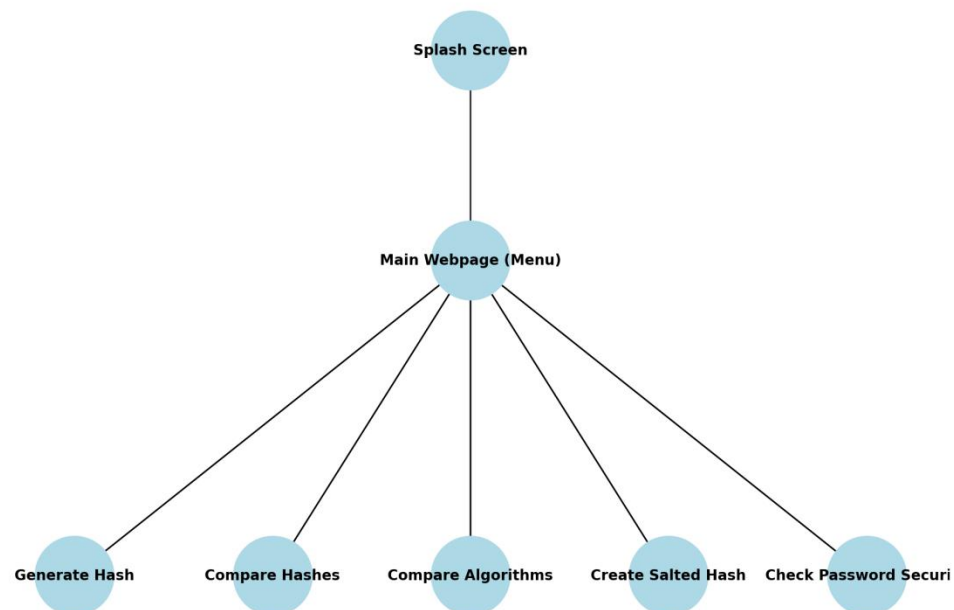
○ **Potential Logo Designs:**

This section includes the potential logo images for the project. These logos will reflect the project's theme of data security, hashing, and professionalism.

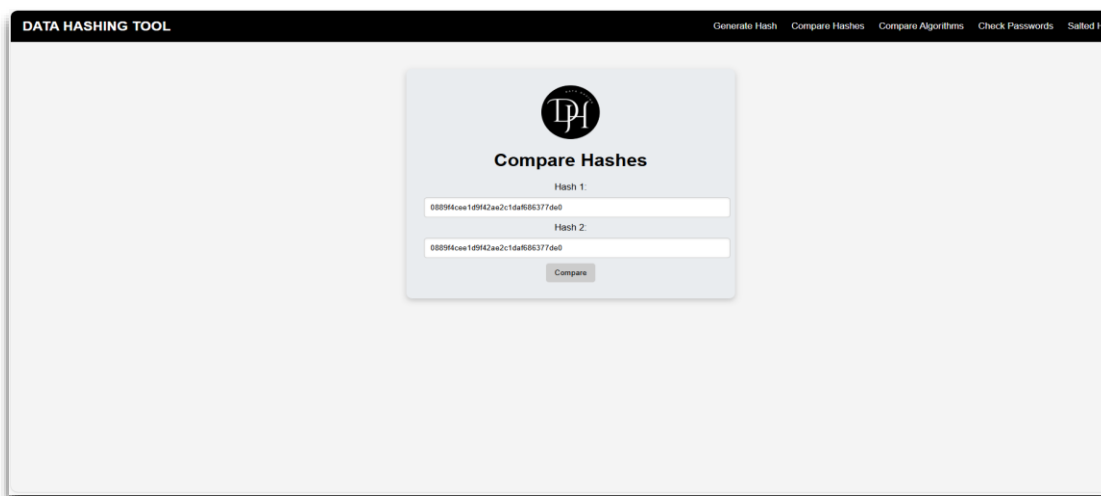


- Flowcharts illustrating the hashing process and the project's architecture.

Project Flowchart: Data Hashing Tool



- Sample screenshots of the user interface:



Project Completion Timeline:

| Phase | Task | Estimated Duration |
|------------------------|--------------------------------------|--------------------|
| Phase 1: Planning | Finalizing features and tools | 2 days |
| Phase 2: Design | Creating logo, splash screen, and UI | 3 days |
| Phase 3: Development | Implementing frontend and backend | 1 week |
| Phase 4: Integration | Merging and testing functionalities | 1 week |
| Phase 5: Documentation | Writing user manuals and reports | 3 days |
| Phase 6: Presentation | Preparing for final submission | 1 week |

Conclusion: The "Data Hashing Tool" is a comprehensive solution for hashing, comparison, and security analysis. It combines theoretical and practical aspects of information security, providing users with a functional and educational experience. This project not only showcases our technical skills but also addresses a significant need in today's data-driven world, making it a valuable and impactful contribution to the field of cyber security.