**Modules Description**

* Dataset Initialization
* Password Strength Analysis
* Shadow Attack Analysis

**Dataset Initialization**

The first module in the design is the dataset initialization module. Here admin is used to process under the specification purposes. The methodology purposes are based upon the web based application criteria. Through which the admin can account the behaviours of the user. The next step is user must register their details under the admin. This is designed for the security purposes. Then admin verify all the details of the user and provide access permission to the user. These details of the user maintained by the database. Dataset design is the next step in this process. The modelled purposes are used to avoid the data set leakage in the system. Here the data set is designed with the clustering and hierarchical process. The clustering is the grouping mechanism was the data are designed with the simple and effective process. The hierarchical model is used to link between the resource and the system. The process usability is used to link between the resource and performance maintenance of the system is used to design. The usage of data set is used to avoid the resource leakage of the user and guarantees the security mechanism.

**Password Strength Analysis**

The next module is Password Strength Analysis. It is mainly designed for the user classification mechanism. The user classification mechanism is designed with the two data set process one is ISPR and the one is CSPR. The ISPR is derived as the Intra site password reuse and the CSPR designed for the cross site password reuse. Thus the performance is used for the simple suffix and prefix model. Utilizing our findings to facilitate password guessing, this project improvement of password guessing success rate. The password strength is analyzed by using password guessing. The password guessing was performed in two ways as online guessing and offline guessing. In online guessing where the adversaries can try limited number of guesses and in offline guessing where the adversaries can guess as many times as possible.

**Shadow Attack Analysis**

The final module is the Shadow attack Quantitative analysis model. This used to concern the methodology or techniques that can be empirically are used for the simple mechanism. The suffix and prefix model is the simple and efficient performance metrics that is designed in the keyboard side which uses SHA1 algorithm. Since the passwords contain less than 2 power 64 bits the SHA1 algorithm is used. The output of SHA 1 message digests. The function of SHA1 algorithm is that is 160 bit in length. SHA- 1 differs from SHA-0 by single bitwise rotation in the message schedule of its compression function to correct the flaw in the original algorithm which had reduced cryptographic security. The SHA1 first get the input as string values which was generated by using keyboard and stored in the buffer then the string values are get converted into byte code and obtain the ASCII value for each byte code and again it was converted into the string then the sixteenth position of string was stored in the first position and they are continuously stored in the reverse order which avoids the hacking of password from the database. Thus this trustfully avoids the shadow attack. In this work the phenomenon of web password reuses (both ISPR and CSPR) is studied guesswork represents the expected number sequential guesses to find the password of an account if an adversary proceeds in an optimal order. And analyze the differences between reused passwords and all passwords. Also the quantitative strength of reused passwords stronger or weaker than any passwords.