File Integrity Checker

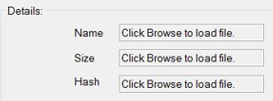
1. The function of file integrity checker is to compare the hash value of a particular file when encrypting it with the hash value of the same file after being received by the recipient to check whether the file has been modified or not. In this case, there is no file transfer function, so we assume that we are the recipient and we are using the file integrity checker to double check the hash value.

2. For example, now we are going to encrypt a file name "**Sample**". Firstly, we will select the **Sample** file from the browse option and also set the file destination. Then a password that meets all the requirements should be entered and also repeat it in confirm password option. Then we click encrypt file option. After clicking encrypt file, the system automatically assigns a unique File ID for **Sample** file like F5516. This unique file ID will be displayed in a pop-up message to the user like "The file ID for **Sample** will be F5516". Then, the system automatically calculates the hash value of **Sample** and stores it in the database with the unique File ID. Like, File ID: F5516 – Hash Value: mndi564165.

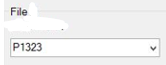
Now when we are going to check the file integrity:

1. We choose **Sample** file from the browse option.

2. The system automatically displays the name of the file, size of the file and recalculate the hash value of **Sample** file and displays it also. Just like in the picture below but the details should be displayed automatically.



3. The user chooses the unique File ID from a drop-down option that displays all the existing File ID that is stored in database, for example, F5548, F5569, F2134. The user then chooses F5516 from the list that’s is being displayed from the drop-down option. Refer to the image below.



4. User clicks the option “Check File Integrity”.

5. Then, the system compares the hash value of **Sample** that has already stored in database when encrypting with the hash value that has been automatically calculated recently in Step 2. If there’s a difference in hash value, a pop-up message saying “File has been modified” should be displayed. If there’s no difference, a pop-up message saying “File has not been modified” should be displayed.

6. To conclude, the hash value is stored based on the unique File ID generated by the system. In this example, the File ID will be F5516. So, the initial hash value of F5516 that has been stored in database after encryption process will be compared with the hash value of F5516 that has been calculated in Step 2. This is to detect whether any changes have been made to the file or not. The unique File ID plays the important role here for comparison.