**MODULES:**

1. **Data Upload**
2. **Multimedia Analysis**
3. **Graph Analysis**
4. **OTP request**
5. **DATA UPLOAD**

The process is initiated in this step and data can be uploaded from the user and admin can be prepare the data to analysis the particular multimedia content is good or not. The multimedia data can be any form of image or so. The data can be stored in the database with the details are given. The main upload part is done with the given folder in django framework. The python frame work allows user to store data.

1. **MULTIMEDIA ANALYSIS**

The Uploaded data then process to this level of project, once user is enter into the data, multimedia pixels were calculated. The pixels are then compared with the given trained data of admin. Admin can train the data with particular amount of data and have set the bench mark for the quality of the content in multimedia.

1. **GRAPH ANALYSIS**

The data can be given to graph in order to analysis. The graph may be varying to analysis particular data. The Pie, bar or line chart are more convenient to do this. The graph data are taken from the analysis section of the process and it can be modified based on the changes done to graph data.

1. **OTP Request**

A **one-time password** (**OTP**), also known as **one-time pin**, is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to *something a person has* (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as something a person knows (such as a PIN).

The most important advantage that is addressed by OTPs is that, in contrast to static [passwords](https://en.wikipedia.org/wiki/Password), they are not vulnerable to [replay attacks](https://en.wikipedia.org/wiki/Replay_attack). This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker