**MODULES:**

1. **PRESCREENING**
2. **THREAT DETECTION**
3. **LIMIT RESOURCES**
4. **ANALYSIS**
5. **PRESCREENING**

Normally the screening process of the system can be done by login system but with this system username and password alone not enough to authenticate the system. The security questions will be set to each user separately in order to make sure the correct user logged in or not. It sets the limit the access of users from threats. The class can be limited by admin while registering and admin alone approve the user’s entry to system.

1. **THREAT DETECTION**

The threat can be detected with the help of prescreening technique. Threats can be illegal access to system with more than five times trying to access the particular account with different act. The Insurance policies can be set to different users. According to policies users can be access. Within certain number of attempts goes wrong the user can be blocked and need to request admin to unblock again.

1. **LIMIT RESOURCES**

Admin is the authorized person to control polices and rules breaches. The wrong access of particular document more than certain number of time that is described in the policy can be blocked by admin and gets the intimation of breaches to admin. Then according to request by admin to user can be block or unblock the resources which are uploaded by admin/user.

1. **ANALYSIS**

The analysis of the system is done in this module. The proposed algorithm’s efficiency is calculated here. The comparison of various factors can be handy to calculate and visualize in the graphs such as pie chart, bar chart, line chart. The data to plot the graph is taken from the system which is done.