Implementation

We have used AWS for implemented of the idea presented.The main idea is suppose IIITG has it's own cloud,there are different groups of users like Instructors, Students, PhDs,HODs, Deans and Director. Each one has a different set of access rights associated with it and should be done in a way that the privacy and security of confidential information is maintained.
Here we're taking the example of Instructor & Student groups. Suppose a instructor uploads course materials time to time in cloud and wants each student to view them , complete and submit. But he doesn't want the materials to be changed or updated or deleted , thereby the rights of students are limited to read only and instructor has all the rights.

1. We have created groups(on based of roles) i.e Instructor and Student.

2. The Instructor has AWS S3 Full Access (One of the rights from the policy), so that he can upload the course materials & update them time to time.

3. The Students has AWS S3 Read Access, so that he could only view the materials and download them, but couldn't upload any materials or delete any pre-existing file.

4. Suppose two students come for registration ,they have been granted the permission and their credentials have been sent to them by the adminstrator through mail.

5. Now, an instructor have been also sent the credentials by adminstrator and the rights have been alloted as mentioned above.

We have used mainly IAM and it's access policies(namely AWS S3 Full Access & AWS S3 Read Access) . The option of verifying the users identity is done when users try to access the AWS management console & after that all the rights he has or not the actions will be permitted or denied.

The Project could be checked by using the credentials mentioned in the credentials.csv file. I have mailed you the credentials of Instructor you can directly use that to open and check the above mentioned rights are working fine or not.