

## Implementation of Databox

Prof. Shabana Sultana<sup>1</sup>, Ms. Naureen Khader Sait<sup>2</sup>, Ms. Shumela<sup>3</sup>, Mr. Saraansh Dayal<sup>4</sup>, Mr. Siddhartha Jha<sup>5</sup>

Department of Computer Science and Engineering

The National Institute of Engineering, Mysore, Karnataka, India

Shabnamkbn2k@yahoo.co.in<sup>1</sup>, naureen\_khader@yahoo.com<sup>2</sup>, shumela2111@gmail.com<sup>3</sup>, saraanshdayal@rocketmail.com<sup>4</sup>, siddharthajha69@gmail.com<sup>5</sup>

**Abstract**— Databox is a file hosting service[1]. It's one of its typical usage is being implemented here as an example. This project implements databox as an online learning portal. This finds the usage across domains. The admin of the website uploads the files in the form of images, videos and PDFs. Only the registered users are allowed to access the material stored in the website. The registered student will have a private key to see the document after decrypting it. The private key will be made available to the registered student after registering into the website.

**Key words:** file-hosting service, AES, Encryption, Decryption

\*\*\*\*\*

### I. INTRODUCTION

Databox is a web application[2] developed for maintaining the course on the basis of students' requests. Here the admin, who is handling the courses, will be responsible to send course to the students. For each student there will be a given account with a separate username and password. An accurate course is uploaded by the admin based on the student's request.

Databox in many educational institutions is a vital aspect of administration and can often become a time consuming, hard job, which lends itself to inaccuracies. By employing an automated system, we are allowing resources to be released to other areas where they can be used more effectively, which in the long-run will save you both time and money.

### II. REVIEW

#### A. Existing Method

The Existing method is a manual entry for the students and courses. Here the courses will be carried out in the hand written registers. It will be a tedious job to maintain the record for the students and courses. The human effort is more here. The retrieval of the information is not as easy as the records are maintained in the hand written registers. This application requires correct feed on input into the respective field. Suppose the wrong inputs are entered, the application resist to work. So the user find it difficult to use.

#### B. Proposed Method

To overcome the drawbacks of the existing system, the proposed method has been evolved. This project aims to reduce the paper work and saving time to generate accurate results from the student's. The system provides with the best user interface.

The efficient reports can be generated by using this proposed system.

Advantages of Proposed method

- It is trouble-free to use.
- It is a relatively fast approach to enter attendance
- Is highly reliable, approximate result from user
- Best user Interface
- Efficient reports

### III. FUNCTIONAL REQUIREMENTS

#### ➤ Admin

- **Login:** admin can login through valid username and password.
- **User registration:** admin can view and accept the user registration request.
- **Course list:** admin will add the list of available courses.
- **Course materials:** admin will upload the course materials like pdf , images, video etc..

#### ➤ User

- **Registration:** user has to register with the require details and select the course from the menu list.
- **Login:** user can login through valid username and password.
- **Course materials:** user can view the course material details like pdf , images, video etc..
- **Logout:** user will be logout.

#### Non-Functional Requirements

Non-functional requirements are constraints that must be adhered to during development. They limit what resources can be used and set bounds on aspects of the software's quality. One of the most important things about non-functional requirements is to make them verifiable. The verification is normally done by measuring various aspects of the system and seeing if the measurements confirm to the requirements. Non-functional requirements are divided into several groups:

The first group of categories reflects the five qualities attributes

- **Usability:** The application which we are developing is going to be used by the customer or the stakeholders. This is going to help them in predicting order of processing books.
- **Efficiency:** Our application takes less time to accomplish a particular task such as placing orders which also reduces time complexity. It reduces the complications when an information has several functionalities thus increases the efficiency.
- **Reliability:** The application that we are developing is designed to deliver set of services as expected by the user. The application provides many modules

and each module is developed satisfy the non functional requirements of the customers.

- **Maintainability:** The application that we are developing is going to provide a high performance measures such as the data updates are done automatically without loss of data that already exists.

These requirements constrain the design to meet specified levels of quality.

The second group of non-functional requirements categories constrains the environment and technology of the system.

#### IV. DESIGN PROCEDURES AND METHODOLOGY

##### A. Use cases

A use case diagram at its simplest is a representation of a user's interaction with the system and depicting the specifications of a use case[3]. A use case diagram can portray the different types of users of a system and the case and will often be accompanied by other types of diagrams as well.

**Use case-** Accessing stored data in databox

**Primary actor-** Admin, user

**Goal in context-** to retrieve the data files stored in the databox through the personal user account

**Preconditions-** This system is equipped with a MySQL database and to recognise user functions

**Trigger-** When user interacts with the system.

**Scenario- Admin :** Observes the admin panel

- : Account activation only if the user's details are authentic
- : Update or delete the files
- : View user functions and approve the requests
- : Account revoke

**Customer:** login to the system and if a new user then register

- : use private key for decryption
- : viewing of account and change the password
- : delete account

**Exceptions-** Password is incorrect.

Password may not reach the user in latency time due to congestion.

There may be no result present in the database for users' search.

**Priority-** Essential, must be implemented

**When available-** Second increment

**Frequency of use-** many times

**Channel to actor-** view main program interface

**Open resource-** Should the file uploaded be public?

Should the user have an option for sharing the files in his account?

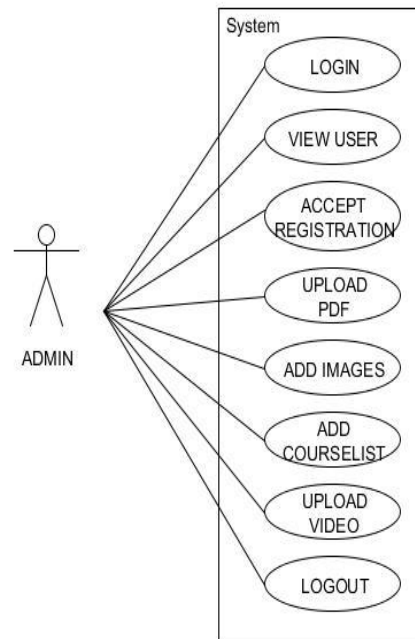


Figure1: Use Case for Admin

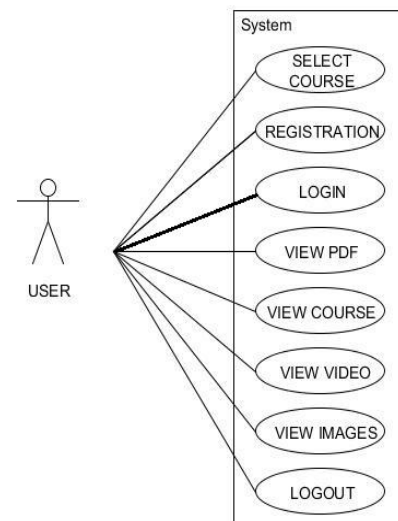


Figure2: Use Case for the user

##### B. Data Flow Diagram

A Data Flow Diagram (DFD) is a graphical representation of the "flow" of data through an information system, modeling its process aspects. A DFD is often used as a preliminary step to create an overview of the system, which can later be elaborated. DFDs can also be used for the visualization of data processing (structured design).

A DFD shows what kind of information will be input to and output from the system, where the data will come from and go to, and where the data will be stored. It does not show information about the timing of process or information about whether processes will operate in sequence or in parallel.

V. FUNCTION MODULES

A. Admin Modules



Figure5: Admin Page

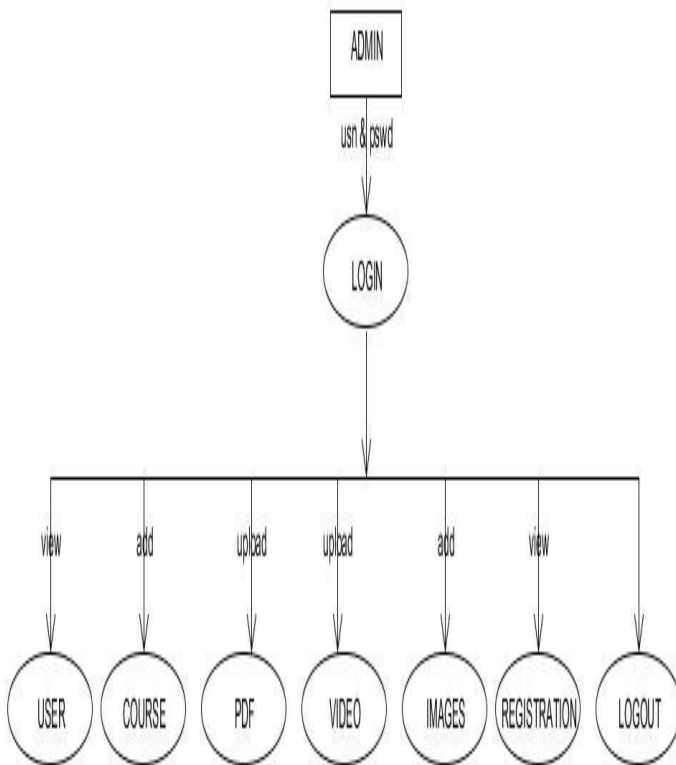


Figure3: DFD for the Admin

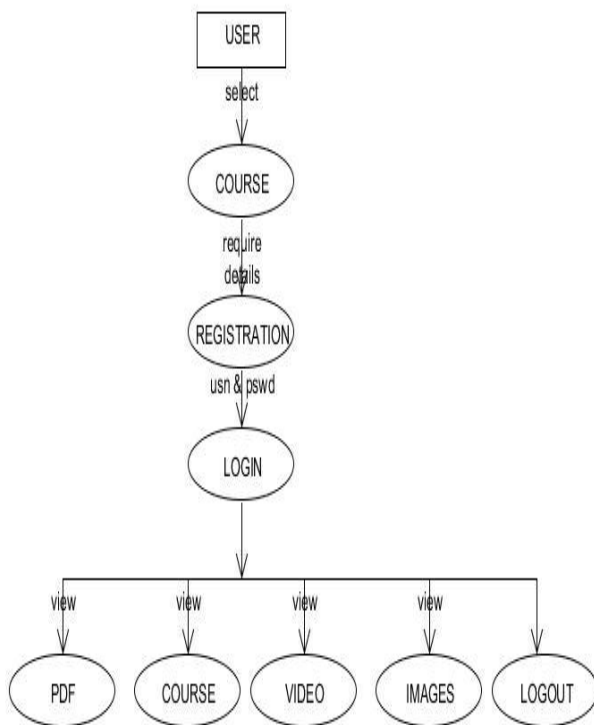


Figure4: DFD for the user

(a) AcceptUser

This module accepts the user by fetching the user id from the database. The user id is submitted into the database after the user submits the details. The private key generated is then sent to the user’s e-mail id. And thus the registration of the user is successful upon acceptance. The message sent to the user contains the private key which is unique for every user. In the database the key is set to the one generated, and the status is set to ‘yes’.

(b) RejectUser

This module rejects the user by fetching the particular user id from the database.. The message generated is then sent to the user’s e-mail id. And thus the deletion of the user account is successful. The message sent to the user informing about account deletion. In the database the key is set to ‘null’, and the status is set to ‘pending’.

(c) UploadFile

This module is used for uploading the file into the database MySQL[4]. This function is carried out by the admin. First line explains the path where the file is used to store. The file permission is set to ‘read’. The ‘request.getParts()’ is used to retrieve the file data part by part. ‘Part.write()’ uploads the file to the specified upload path.

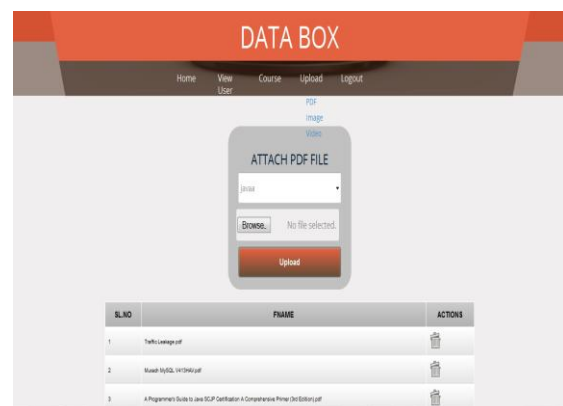


Figure6: File Upload page on admin’s page

A. User modules

(a) ValidateFile

This module is used for the validation of the user key. If the key is correct the 'if(rs.next())' loop is executed and the file is viewed. If the key is wrongly entered then the message 'wrong key' is displayed and the file does not show.

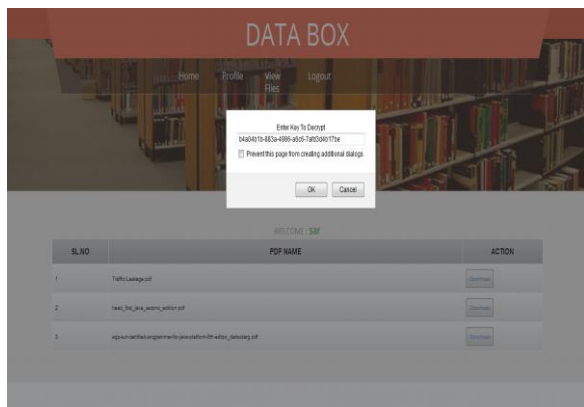


Figure7: usage of the key to decrypt the files

C. Source Package modules

(a) AddCourse

This module is aimed at adding the course to the website. Course with the status isactive = '1' is added and the parameter is passed to the function. The 'rs' object takes it in and checks if it already exists. If it does not then the course is added. Else the message 'already exists' is displayed.

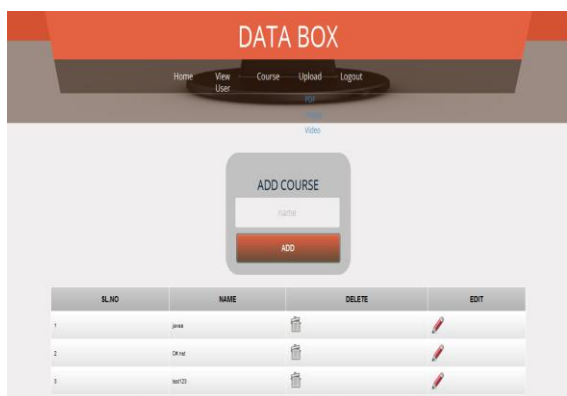


Figure8: Add course page

(b) GetPass

The GetPass.jsp file is used to generate the random private key for each user. Here we specify the upper bound as 10000 and the lower bound for the random key as 5. The random number generated is stored in the String type num which is then type casted to a String type uuid.

(c) SendMail

SendMail is used to send user the mail containing the private key generated. The string host is the e-mail id sending the private key. The mail server is set up first. Then

the default session object is fetched. Eventually the confirmation is sent followed by the private key and the message showing 'thank you'.

(d) AdminLogin

AdminLogin file takes in the username and the password. Prepared statement object 'stmt' sets the query to fetch the username and the password. This is then stored in the ResultSet object 'rs'. This 'rs' is used to access the database and authenticate the admin details. if correct then it redirects to the admin page, else 'invalid entry' message is displayed.

(e) UserLogin

First the connection is set up. Then the query to fetch the username and password of the user is executed. Then it's existence is checked using the object 'rs' with the help of 'rs.next()'. If it exists then the user page is redirected. If it does not exist then the message 'invalid entry' is shown.

D. Modules functioning and sequence

The modules are written and connected using Java[4] programming language. The user registers by creating a new account. The user then logs-in into his account which is enabled by 'UserLogin' module. The admin then after logging in through 'AdminLogin' module views the user. He can accept or reject the user through 'AcceptUser' or 'RejectUser' modules respectively. If the admin accepts the user's registration then he receives a mail stating his confirmation of registration through the 'SendMail' module. Next the 'GetPass' module generates the random private key which is sent to the user through the mail. The admin also adds the required course through the 'AddCourse' module. The admin uploads the file into the particular course using the 'UploadFile' module. Next the user can view the files in the portal after downloading them which is enabled by 'ValidateFile'. This module works using the key generated for every user. The key is used by the user to view the downloaded files.

VI. ADVANTAGES

- 1) The private key generated after the user's successful registration helps in decrypting the encrypted files. This ensures security of the files.
- 2) No random person accessing the files through someone else's account can view the files. This is because of the private key which is unique for every user and is sent to the user's e-mail id secretly.
- 3) This proposed system helps the students to collect the study materials at one place. The student does not have to run for Xerox notes and buying materials.
- 4) Users' registration processes are successful only when they are approved by the admin.

VII. CONCLUSION

The proposed method helps student in the educational institutions to access the required study materials at one common place. The students do not have to spend energy in running around and collecting Xerox notes and other required materials. This system also ensures complete

security by providing each user with a private key. This key is used by the user to view the files after downloading. If the key is not used then the files can be viewed even after downloading due to their encrypted form. The key is therefore used to decrypt the files. Thus, any random person not related to the institution cannot view the files through someone else's account to view the files. In this system AES(Advanced Encryption Standard)[6] 128 bit encryption algorithm [7] is used to encrypt the stored files.

#### VIII. FUTURE ENHANCEMENTS

- 1) The current system's domain can be increased from the particular institution to the university encompassing many colleges affiliated to the university.
- 2) The domain can also be changed and be deployed across different business sectors.
- 3) It can be used in the companies' offices for the important files to be accessed only by the members of that company.
- 4) Thus, the current system's usage can be extended from e-learning portal for a particular institute to confidential file storage system across different business sectors and industrial offices.

#### REFERENCES

- [1] [http://en.m.wikipedia.org/wiki/File\\_hosting\\_service](http://en.m.wikipedia.org/wiki/File_hosting_service)
- [2] <http://www.w3school.com/>
- [3] <http://searchsoftwarequality.techtarget.com/definition/usage-case>
- [4] Java complete reference by Herbert schildt, 9<sup>th</sup> edition, Oracle press, McGrahill Education
- [5] <https://www.mysql.com/>
- [6] Cryptography and Network Security, Behrooz Forouzan, SIE, 2<sup>nd</sup> Edition, McGraw-Hill
- [7] <http://www.networksorcery.com/enp/data/encryption.htm>