Software Design Document (SDD)

**Project Name: IDENTITY-BASED ENCRYPTION USING KEY UPDATE-CSP**

**Name: Prabhunath Yadav**

**Reg No: 1031210334**

**Name: Ashish jangu  
Reg No: 1031210332**

**Project Guide: Mr. M. RAJASEKARAN**

Date: Jan 8 2016.

|  |  |  |
| --- | --- | --- |
|  |  | Software Design Document |
| **TABLE OF CONTENTS** | |  |
| **1.** | **INTRODUCTION** | **2** |
| 1.1 | Purpose | 2 |
| 1.2 | Scope | 2 |
| 1.3 | Overview | 2 |
| 1.4 | Reference Material | 2 |
| 1.5 | Definitions and Acronyms | 2 |
| **2.** | **SYSTEM OVERVIEW** | **2** |
| **3.** | **SYSTEM ARCHITECTURE** | **2** |
| 3.1 | Architectural Design | 2 |
| 3.2 | Decomposition Description | 3 |
| 3.3 | Design Rationale | 3 |
| **4.** | **DATA DESIGN** | **3** |
| 4.1 | Data Description | 3 |
| 4.2 | Data Dictionary | 3 |
| **5.** | **COMPONENT DESIGN** | **3** |
| **6.** | **HUMAN INTERFACE DESIGN** | **4** |
| 6.1 | Overview of User Interface | 4 |
| 6.2 | Screen Images | 4 |
| 6.3 | Screen Objects and Actions | 4 |
| **7.** | **REQUIREMENTS MATRIX** | **4** |
| **8.** | **APPENDICES** | **4** |

**1. INTRODUCTION**

**1.1 Purpose**

The purpose of the Software Design Document (SDD) is to provide a description of the design of a Identity Based Encryption using Key Update Cloud Service provider, fully enough to allow for software development to proceed with an understanding of what is to be built and how it is expected to be built. The Software Design Document provides information necessary to provide description of the details for the website and system to be built.

**1.2 Scope**

This (SDD) Software Design Document is focused on the base level system and critical parts of the system such as security. For this particular Software Design Document, the focus is to user upload their data and share in a secured manner. The website will be used in conjunction with other pre-existing systems and will consist largely of a platform for effective encryption and decryption that is using RSA Algorithm and the system designed using the J2EE (JSP,Servlet,MySql).

**1.3 Overview**

This SDD document describes the major design structure of our Identity Based Encryption using Key Update CSP project. It manages the user profile and data on server , for security purpose it does encryption and decryption using RSA Algorithm , It mainly reduces the over load functionality of PKG(Private key generator).

**1.4 Reference Material**

-Software Requirements Specification

Requirement Description Design Reference

1. Inputs as file.

2. Cloud Services to act as storage point.

3. Keys (Public and Private)

4. RSA Algorithm

5. Database for PKG and CSP

6. User Profiles documents.

7. Session maintenance

8. Revoked list and Time list

9. Finalizing

**2. SYSTEM OVERVIEW**

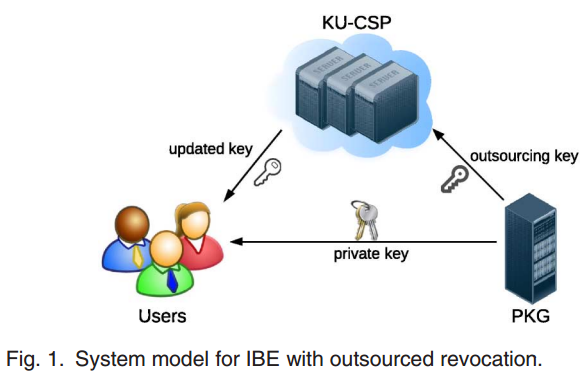
The general description of the priority, functionality, context and design of our project. The whole system is realized using the Java 2 Extended Edition , MySql, RSA Algorithm , HTML , CSS , Java Script and Cloud Services.

**3. SYSTEM ARCHITECTURE**

**3.1 Architectural Design**

This is the layout of project representing every modules with their functionality of the system . It is a high level overview of how users data will be managed , encryption and decryption and sharing and generation of public and private key. That gives a basic understanding and structure of how Website will work.

This is given the following diagram:



**3.2 Decomposition Description**

1. User:

-Self Registration

-Upload Files

-Request for access on cloud

-Request for file Key access.

-Request for key to decrypt the data

-Updates files.

-Logout Account

2.PKG:

-Checks Database updating.

-Maintains users file public key

-Generates first private key.

-Notify to CSP for public key and encrypted data.

-First key generated to authorized users.

3.CSP :

-Maintains Revoked List and Time List

-Generates key for files

-Listens Users Request for key generation.

-Displays the file name.

-Provide key using Email to user.

-Encrypted data is stored.

-Displaying the date of upload and user details.

**3.3 Design Rationale**

The rationales for the design described in 3.1 are:-

* Have a simple division of roles of User , PKG and CSP.
* Have set of activities that are simple to understand and execute
* Have a structure that is easy to maintain and update
* Have a structure that has the ability to have additions in the future
* Provide autonomy to the whole system
* Encryption and decryption based on RSA Algorithm.

**4. DATA DESIGN**

**4.1 Data Description**

Tables Used:

| **Table** | **Rows** | **Type** | **Size** |
| --- | --- | --- | --- |
| **pkg** | 0 | InnoDB | 0 KiB |
| **csp** | 0 | InnoDB | 0 KiB |
| **users** | 0 | InnoDB | 0 KiB |
| **Users\_files** | 0 | InnoDB | 0 KiB |
| **5 tables** | **0** | **--** | **0 MiB** |

**4.2 DATA DICTIONARY**

A data dictionary is a collection of the data objects or items in a data model for the benefit of programmers and others who need to refer to them.

* Achievements -Lists the rewards/certificates received by the user so far by competing in contests conducted by this website.
* Area Of Interest -Lets the user to select the area of interest in which he/she wish to upload the document.
* Security -Encryption and Decryption.
* Algorithm -RSA
* Database –Holds relevant data and documents.
* New User -User who has not created an account in the website so far.
* Password -Security Code.
* Storage –Structured data.
* Registered User -User who has an existing account already in our website.
* Key Size -1024bit.
* Sign In -Enter into registered account.

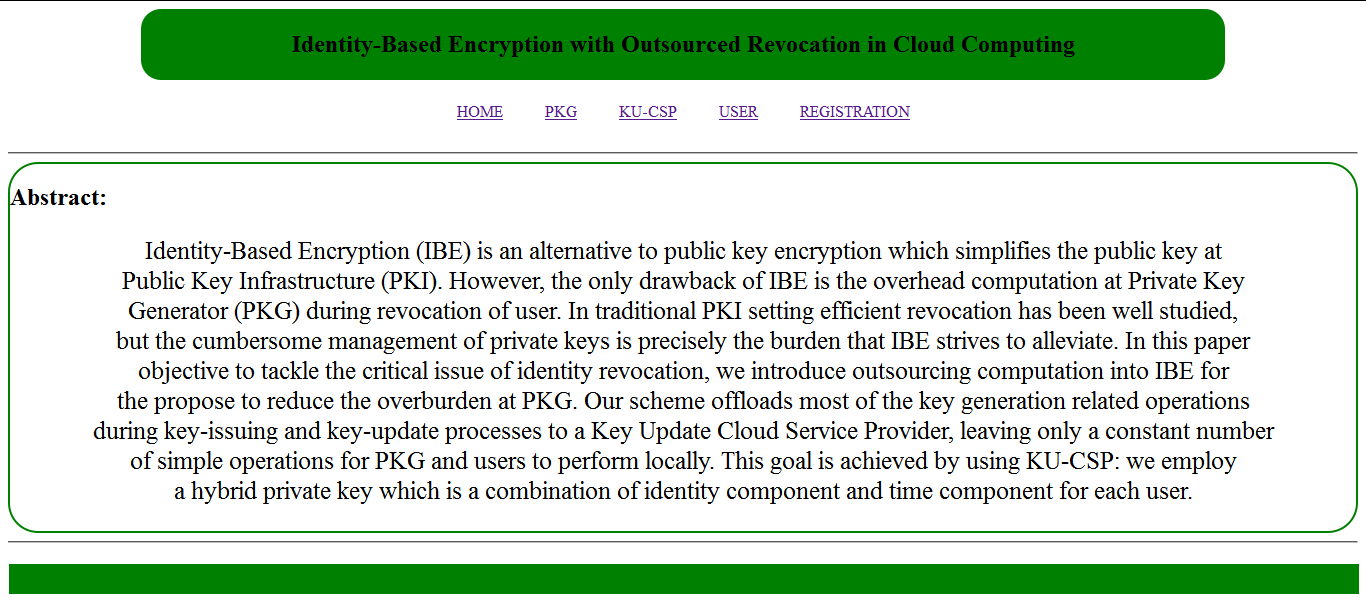
**5. COMPONENT DESIGN**



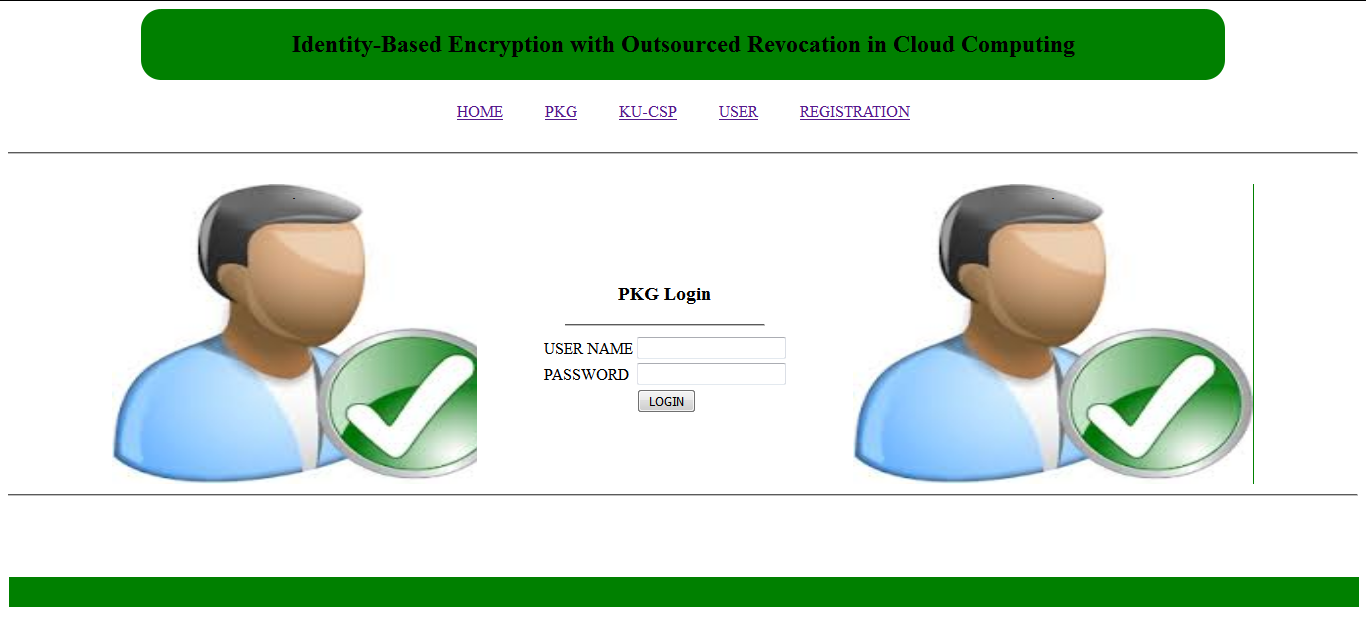
**6 .0 HUMAN INTERFACE DESIGN**

Screen Images

**6.1 Index**



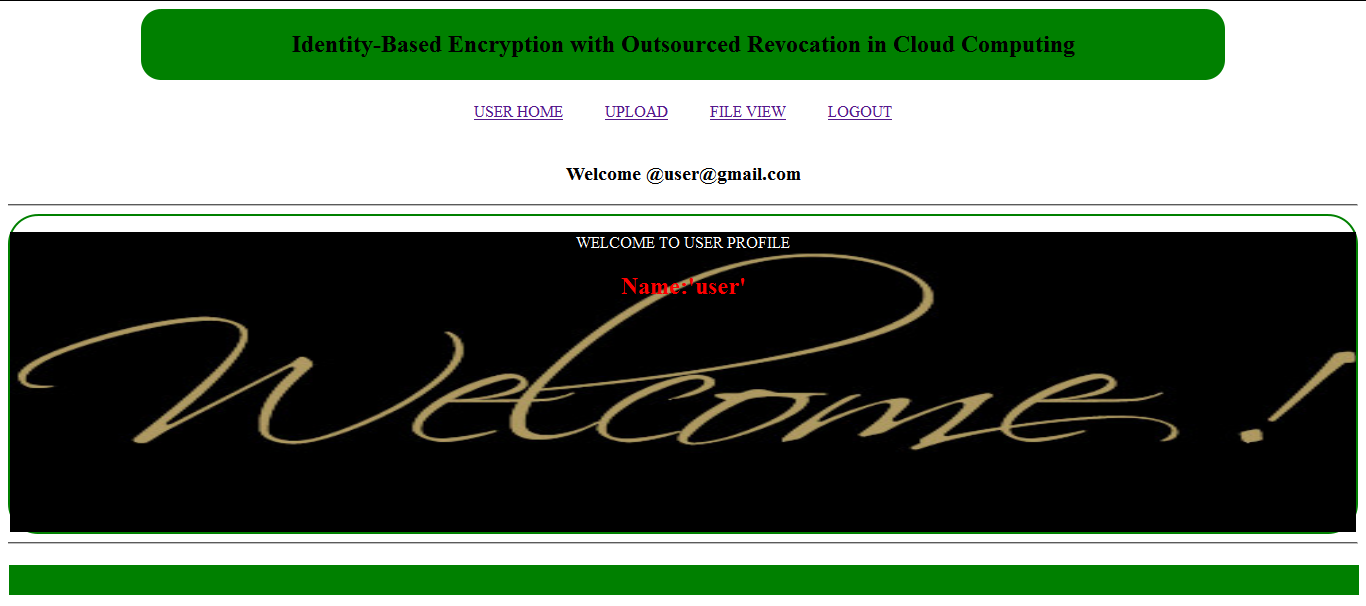
PKG Login



**KUCSP LOGIN**

**6.2 User Registration:** ****

**6.3 User\_ Profile**



**7. REQUIREMENTS MATRIX**

| **Feature** | **Requirements for Simple users** | **Requirements for the CSP, PKG** |
| --- | --- | --- |
| * **Register the User** | *Register self on the website using a registeration form, enabling the user to upload their documents.* | *Maintain a database for the registered users and their details to PKG and CSP Holds encrypted data.* |
| * **View the Documents** | *Users should be able to view their documents and what the detail they have given.* | *Enables PKG to generate key for file and CSP can update the data.* |
| * **CSP Services** | *Key update and allows for services.* | *Maintains revoked list and time list.* |
| * **PKG Services** | *First key is generated.* | *CSP updates the keys for encryption and decryption.* |
| * **Users Document** | *Allows to upload on database.* | *Able to encrypt and decrypt* |
| * **Login** | *Verified User can only login access* | *CSP and PKG must validate the user and provide the allow access.* |
| * **Registration** | *User can only register by filling up the relevant information such as name , email, phone number , location* | *All the user details will be notified to CSP and PKG.* |

**8.APPENDICES:**

**Appendix A:**

**Importance:**

Purpose of SDD is to provide a description of design of J2EE based Websites, understanding information necessary to provide description of the details for the software and system to be built.

Software Design Document, the focus is placed on the basic structure of the course website. The system will be used in conjunction with other pre-existing systems and will consist largely of a platform for effectively delivering online course material through a system designed using the J2EE tools.

**Appendix B:**

**Architectural design:**

It is the modular program structure and the relationships between the modules to achieve the complete functionality of the system, decomposition description interrelates the modules and makes proper functionality.

Data Design and descriptor:

It declares or represents the specific terms which is going to be used in the modules with their specific property.

**Appendix C:**

Interrelating each components with their functionality is represented by Component Design .

Human Interface Design represents all the front-end activities that a user is going to access the application and it’s a proper layout view which may consist of user documents like .txt , .doc , etc files format.

Requirement matrix: It is a matrix form details of the application representing features ,requirements , Algorithms and the interaction between User, CSP , and PKG.