ISSN: 2366-1313

# DIGITAL CERTIFICATE MANAGEMENT SYSTEM

[1]Mrs.SWETHA.G, [2]J.BHAVANA, [3]K.NARESH, [4]M.NIKITHA

[1](Assistant Professor) ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

[234]B,tech scholar ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

## ABSTRACT

Digital Certificate Management system is to encourage advanced issuance, capacity, get to and confirmation of Scholastic Grants issued by Scholastic Teach. DCM could be a Interesting, Inventive and Dynamic activity beneath "Digital India" subject towards accomplishing in the by Computerized enablement of the Instruction Records. DCM aims to form the vision of Advanced Scholastic Certificates for each Indian a reality. This touches the lives of Indian youth and enables them with Advanced, Online, Trusted, Irrefutable Certificates which are open in a secure way at all times. DCM guarantees to do absent with troubles / inefficiencies of collecting, keeping up, and showing physical paper certificates.

- The Scholarly Educate hold up the points of interest of the scholarly records within the store framework;
- The understudies get to their certificate records in their accounts which are kept up within the vault framework;
- The confirmation clients I.e. banks, managers, scholarly teach access the depository

## 1.INTRODUCTION

DCM could be a Special, Inventive and Dynamic step towards accomplishing computerized enablement of Instruction Records. DCM will create an internet portfolio of all instruction certificates over Scholarly Establishing (Colleges / Organizing / Sheets) which can be submitted effectively for work, higher instruction, and advance and is effortlessly trusted and confirmed. DCM coordinating straightforwardly with Sheets / Colleges which issue Certificates and consequently guarantees Realness of Certificate Records.

DCM will give a innovation edge to scholastic teach.

They can issue and keep up all their records in electronic arrange without causing venture, costs and support endeavors. College / Sheets will straightforwardly hold up the scholastic grants in DCM framework in a secure online handle. DCM brings in a solid discouragement component within the frame of online unquestionable status and consequently makes a difference to dispense with fake and produced certificates. DCM will create a web portfolio of all instruction certificates for each Citizen over Scholarly Educate (Colleges / Sheets / Evaluation Bodies) which can be submitted effectively for work, higher instruction, and advance and is effectively trusted and confirmed. DCM will be an dynamic online put for Understudies, Scholarly. DCM will be an active online place for Students, Academic Institutions and Verification Users. DCM brings in deterrence factor for people who wish to think that paper certificates can be easily forged / created and as verification processes are costly and inefficient they can use the arbitrage. By doing so it also brings trust and credibility to genuine certificate holders and makes their certificates trusted and easily accepted.

## 2.LITERATURE SURVEY

These days ICT 6 is being utilized in several electronic components like E Governance, ELearning, E-Shopping, E-Voting, etc. The victory rate of these instrument are completely subordinate on the security, authenticity and the judgment of the data that's being transmitted between the clients of sending conclusion and the clients of accepting conclusion amid execution of the Eservices. To accomplish all these parameters, the delicate data must be carefully marked by its genuine sender which ought to be confirmed by its aiming beneficiary. The Advanced Signature is essentially a scientific usage of topsy-turvy cryptographic strategy over the digitized record to guarantee its genuineness and judgment to its clients. Its concept is exceptionally much comparative with the routine marks which are utilized to prove the root of the record so that a beneficiary encompasses a reason to accept that the message was created by the real sender and was not misshaped amid the travel. The Computerized Marks are utilized to attain verification 3 non-repudiation and keenness over the computerized information. –

i.Key generation algorithm.

ii.Signing algorithm.

ISSN: 2366-1313

iii. Signature verification algorithm.

In cryptography, a Key9,10 could be a imperative parameter which is utilized to determine the useful yield of a cryptographic calculation i.e cipher content. Key era is the method of producing keys which are utilized either in symmetric key or topsy-turvy key cryptographic methods. As the symmetric key calculation employments a single shared key, success proportion of the whole cryptosystem depends on the mystery of that key. In differentiate to symmetric key calculation, the hilter kilter key calculation employments a open key and a comparing private key, among which the public key is made transparently accessible to the clients. Within the key era calculation beneath the advanced signature conspire, the private key is haphazardly chosen from a bunch of likely private keys. This sub process at long last produces the private key and the comparing open key. The marking calculation is the moment stage of the advanced signature conspire.

After this stage is over, the sender transmits the message in conjunction with the signature to the recipient. The signature confirmation calculation, which is the third and final stage of the computerized signature plot, is executed at the recipient's conclusion. The collector collects the message and signature transmitted by the sender and gets its open key accessible openly to confirm the signature of the gotten message. In case the signature gotten matches with the signature calculated, the realness and astuteness of the message is set up else it is denied. The success rate of this entire mechanism highly depends on its two prime properties –

i.The signature generated from a specific message and fixed private key should verify the authenticity of that particular message by using the corresponding public key. ii.The procedure must be computationally infeasible to generate a valid signature for an intruder who does not possess the private key. Furthermore, the Digital Signature Schemes can be broadly categorized into - i. Direct Digital Signature – in this technique, the communication is done only between the sender and the receiver of message, assuming that - a. Receiver knows the public key of the sender. The marked message sent by the sender to begin with comes to the arbiter, who performs different security investigation of the message to affirm its beginning and substance and after that it sends the marked message to the collector demonstrating that it had as of now been confirmed. As per the need of digital signature is concerned, it is conceptually same with the ordinary marks, i.e to verify as well as to guarantee the keenness of the archive after being transmitted from the sender's side to the receiver's side. b. Signature can be generated either by encrypting the entire messages with the sender's private key or encrypting hash code of message with sender's private key. c. Confidentiality of the information can be enhanced by encrypting the signed message either with public key of the receiver or by using the shared private of sender and receiver.

The main problem with this technique is that the success rate of this scheme is totally dependent on the security of the sender's private key. ii.Arbitrated Digital signature – in this technique, the communication is done between the sender and receiver of the message via the trusted third party i.e arbiter. 4 The signed message sent by the sender first reaches the arbiter, who performs various security analysis of the message to confirm its origin and contents and after that it sends the signed message to the receiver indicating that it had already been verified. As per the necessity of digital signature is concerned, it is conceptually same with the conventional signatures, i.e to authenticate as well as to ensure the integrity of the document after being transmitted from the sender's side to the receiver's side. It is additionally conceivable to impose integrity of the archive by applying different encryption techniques. But the dis advantage of scrambling the complete document is, it is infeasible with regard to taken a toll, time and asset. In advanced signature method, a message process i s computed using the message and a few standard hash capacities, which is utilized to produce the digital signature. In this way,

the encryption of whole archive is maintained a strategic distance from in this way. The digital signature plans are helpless to different assault models like – i. Key as it were assault, where the assailant has get to the open confirmation key as it were. ii. Known message assault, where the aggressor has get to substantial marks of assortment of messages. ii.Versatile chosen message assault, where the aggressor learns the marks on arbitrary messages of possess choice. Separated from the over specified assaults, the carefully marked records are moreover powerless to other assaults like, widespread fraud assault, particular imitation assault, existential forgery assault. In spite of the fact that there are a few standard computerized signature schemes, of which all of them are not so proficient to handle all these assaults.

This can be since the efficiency figure of these computerized signature plans are dependent on its key size, computational handle, hash work utilized, etc. Within the way to evolution of proficiency and reasonableness in different electronic component, the advanced signature procedures have improved day by day and had at last combined with elliptic bend cryptographic methods to produce ECDSA from DSA, ECEI Gamal from ElGamal, etc. Once the information is marked carefully, E-Governance component transmit it from the sender to it intended recipient using the Data and Communication Innovation (ICT). In this paper the creators have made a intensive think about of the industry standard computerized signature plans to obtain ideal security level for the electronic components and have investigated its plausible applications in different spaces.

## 3.SYSTEM DESIGN

System design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. It involves translating user requirements into a detailed blueprint that guides the implementation phase. The goal is to create a well-organized and efficient structure that meets the intended purpose while considering factors like scalability, maintainability, and performance.

### 3.1 SYSTEM ARCHITECTURE

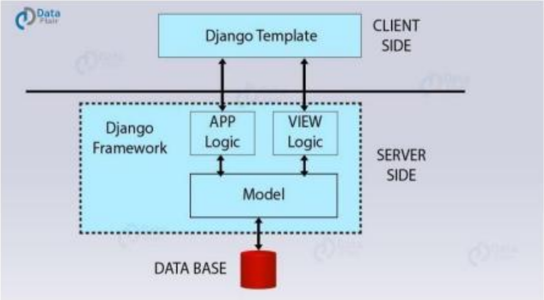
Django is based on MVT (Model-View-Template) design. MVT could be a computer program plan design for creating a web application. MVT Structure has the taking after three parts :

**Demonstrate:** Show is getting to act as the interface of your information. It is capable for keeping up information.

It is the consistent information structure behind the complete application and is spoken to by a database (for the most part social databases such as MySql.

**See:** The See is the client interface — what you see in your browser after you render web site. It is spoken to by HTML/CSS/JavaScript and Jinja records. To check more, visit – Django Sees.

**Format:** A format comprises of inactive parts of the specified HTML yield as well as a few uncommon language structure portraying how energetic substance will be embedded. To check more, visit – Django Templates



### 3.2 ACTIVITY DIAGRAM:

**Purpose:** To depict the flow of activities or processes within a system

**Activity:** Represents a unit of work in the system.

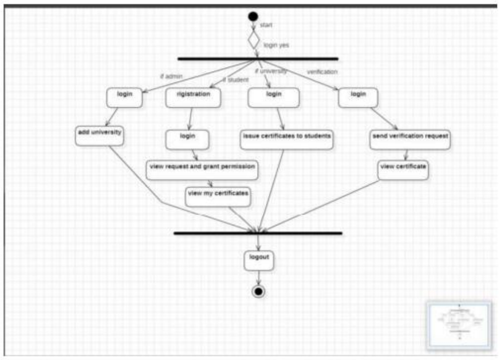
**Action:** Represents a specific operation or computational step.

**Decision Node:** Represents a point in the flow where a decision is made.

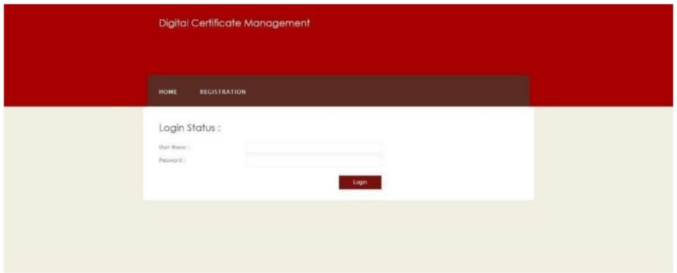
**Control Flow:** Represents the flow of control between activities.

**Fork and Join Nodes:** Indicate parallel or concurrent activities.

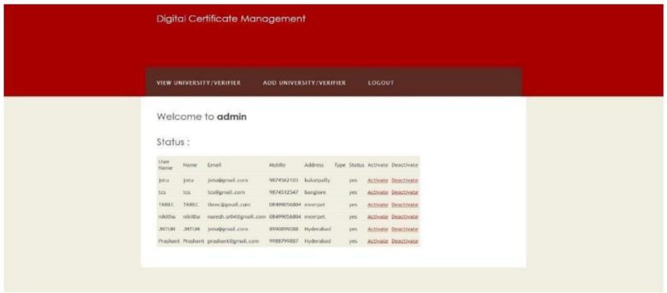
**Initial and Final Nodes:** Mark the start and end points of the activity diagram.



## 4.OUTPUT SCREENS



Here is the first page of the website called Digital Certificate Management System. The page reflects the login page and it has same dashboard for all the modules.



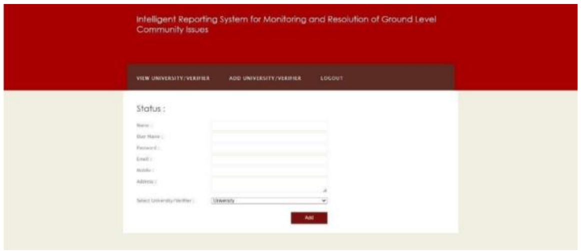
Welcome to **admin**

Status :

| User Name | Name | Email | Mobile | Address | Type | Status | Activate | Deactivate |
|---|---|---|---|---|---|---|---|---|
| jntu | jntu | jntu@gmail.com | 9874562103 | kukatpally | | yes | Activate | Deactivate |
| tcs | tcs | tcs@gmail.com | 9874512547 | banglore | | yes | Activate | Deactivate |
| TKREC | TKREC | tkrec@gmail.com | 08499056804 | meerpet | | yes | Activate | Deactivate |
| nikitha | nikitha | naresh.sr04@gmail.com | 08499056804 | meerpet | | yes | Activate | Deactivate |
| JNTUH | JNTUH | jntu@gmail.com | 8990899088 | Hyderabad | | yes | Activate | Deactivate |
| Prashant | Prashant | prashant@gmail.com | 9988799887 | Hyderabad | | yes | Activate | Deactivate |

Firstly, the admin is logged into the DCM and adds the university/colleges. The admin will verify the details of university and accept it into DCM. Admin has all the login data information such as student,verifier.

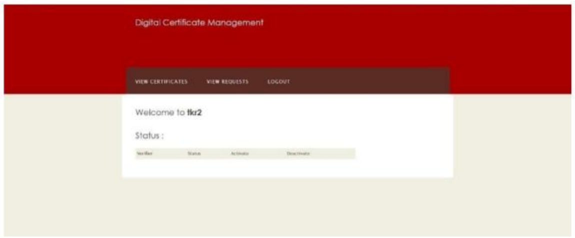
## UNIVERSITY MODULE


Intelligent Reporting System for Monitoring and Resolution of Ground Level Community Issues

Status :

Name :
User Name :
Password :
Email :
Mobile :
Address :
Select University/Verifier : University

Such as Universities / Boards / Academic Institutes / Assessment Bodies as are identified by MHRD / UGC will join DCM system & facilitate students to register on DCM. In this universities will upload the degree certificates of academic.

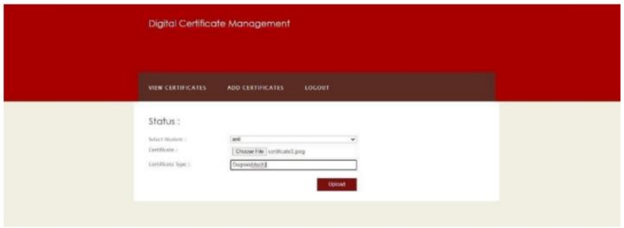

Digital Certificate Management

Welcome to **tkr2**

Status :

| Verifier | Status | Activate | Deactivate |
|---|---|---|---|

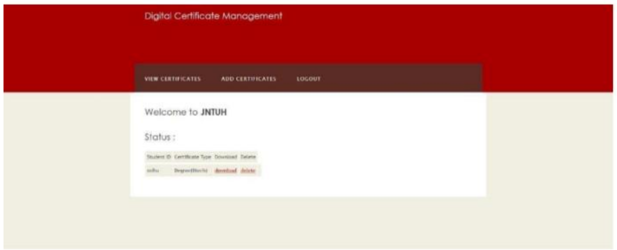
Here is the page of uploaded certificates to students & students can view their all academic certificates.


Digital Certificate Management

Status :

Select Student : anil
Certificate : Choose File certificate3.jpeg
Certificate Type : Degree(btech)

In this the universities will upload the certificates of degree academics and provide digital view to the students.


Digital Certificate Management

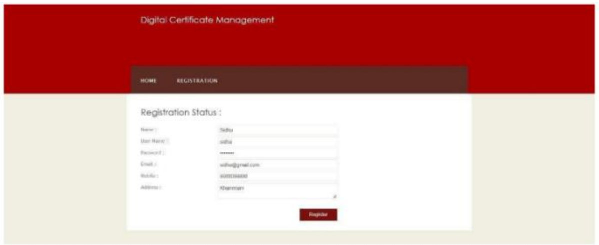
Welcome to **JNTUH**

Status :

| Student ID | Certificate Type | Download | Delete |
|---|---|---|---|
| sidhu | Degree(Btech) | download | delete |

Here it shows the data of uploaded certificates to the students giving the options as download and delete.

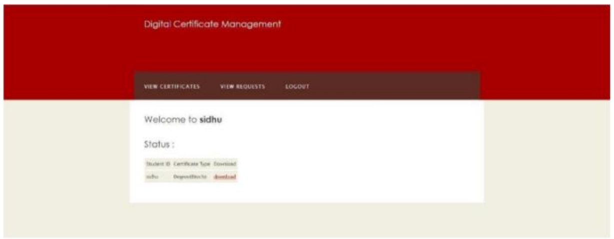
## STUDENT MODULE


Digital Certificate Management

Registration Status :

Name : Sidhu
User Name : sidhu
Password : ••••••••
Email : sidhu@gmail.com
Mobile : [illegible]
Address : Khammam

Here this page provides registration form of DCM to the students to fill the details such as user name, email, password as adhar number and address.


Digital Certificate Management

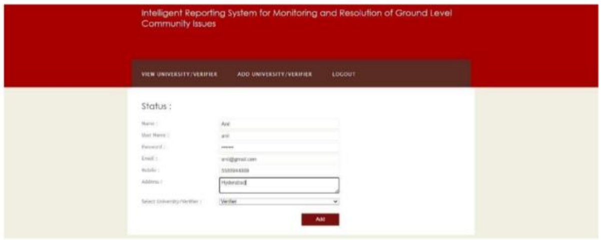
Welcome to **sidhu**

Status :

| Student ID | Certificate Type | Download |
|---|---|---|
| sidhu | Degree(Btech) | download |

After student registration they can view their certificates digitally by downloading the degree certificates.

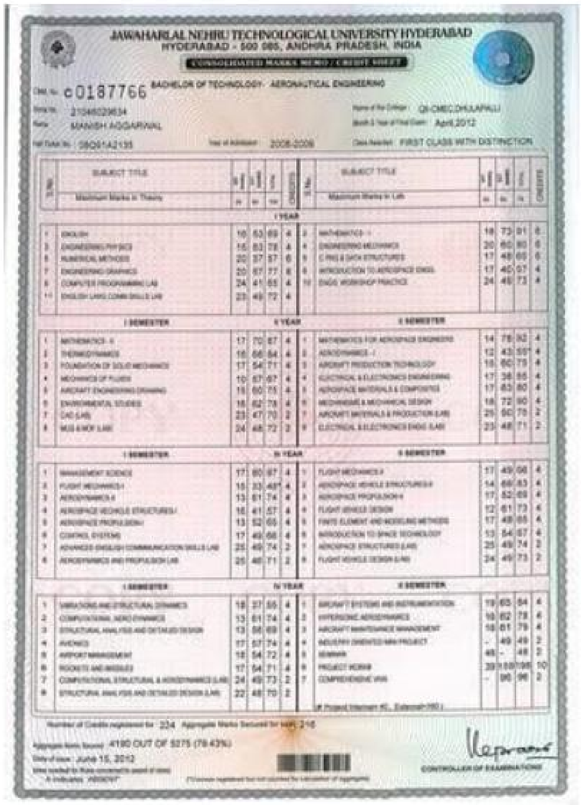
### VERIFIER MODULE


Intelligent Reporting System for Monitoring and Resolution of Ground Level Community Issues
VIEW UNIVERSITY/VERIFIER
ADD UNIVERSITY/VERIFIER
LOGOUT
Add

Status :

Name : Anil
User Name : anil
Password : ******
Email : anil@gmail.com
Mobile : [illegible]
Address : Hyderabad
Select University/Verifier : Verifier

In this a person/organisation/bank/company is logged in as verifier to verify the certificates. And send the request message to the certificate holders.



JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
HYDERABAD - 500 085, ANDHRA PRADESH, INDIA
CONSOLIDATED MARKS MEMO / CREDIT SHEET

c0187766 BACHELOR OF TECHNOLOGY - AERONAUTICAL ENGINEERING

[illegible] 2104602934
Name: MANISH AGGARWAL
Hall Ticket No.: 08Q91A2135
Year of Admission: 2008-2009
Name of the College: QI-CMEC,DHULAPALLI
Month & Year of Final Exam: April,2012
Class Awarded: FIRST CLASS WITH DISTINCTION

| S.No. | SUBJECT TITLE | | | | CREDITS | S.No. | SUBJECT TITLE | | | | CREDITS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Maximum Marks in Theory | | | | | | Maximum Marks in Lab | | | | |
| | | | | I YEAR | | | | | | | |
| 1 | ENGLISH | 16 | 53 | 69 | 4 | 2 | MATHEMATICS - I | 18 | 73 | 91 | 6 |
| 3 | ENGINEERING PHYSICS | 16 | 62 | 78 | 4 | 4 | ENGINEERING MECHANICS | 20 | 60 | 80 | 6 |
| 5 | NUMERICAL METHODS | 20 | 37 | 57 | 6 | 6 | C PRG & DATA STRUCTURES | 17 | 48 | 65 | 6 |
| 7 | ENGINEERING GRAPHICS | 20 | 57 | 77 | 6 | 8 | INTRODUCTION TO AEROSPACE ENGG. | 17 | 40 | 57 | 4 |
| 9 | COMPUTER PROGRAMMING LAB | 24 | 41 | 65 | 4 | 10 | ENGG. WORKSHOP PRACTICE | 24 | 49 | 73 | 4 |
| 11 | ENGLISH LANG COMM SKILLS LAB | 23 | 49 | 72 | 4 | | | | | | |
| | I SEMESTER | | | II YEAR | | | II SEMESTER | | | | |
| 1 | MATHEMATICS - II | 17 | 70 | 87 | 4 | 1 | MATHEMATICS FOR AEROSPACE ENGINEERS | 14 | 78 | 92 | 4 |
| 2 | THERMODYNAMICS | 16 | 68 | 84 | 4 | 2 | AERODYNAMICS - I | 12 | 43 | 55* | 4 |
| 3 | FOUNDATION OF SOLID MECHANICS | 17 | 54 | 71 | 4 | 3 | AIRCRAFT PRODUCTION TECHNOLOGY | 15 | 60 | 75 | 4 |
| 4 | MECHANICS OF FLUIDS | 10 | 57 | 67 | 4 | 4 | ELECTRICAL & ELECTRONICS ENGINEERING | 17 | 38 | 55 | 4 |
| 5 | AIRCRAFT ENGINEERING DRAWING | 15 | 60 | 75 | 4 | 5 | AEROSPACE MATERIALS & COMPOSITES | 17 | 63 | 80 | 4 |
| 6 | ENVIRONMENTAL STUDIES | 16 | 62 | 78 | 4 | 6 | MECHANISMS & MECHANICAL DESIGN | 18 | 72 | 90 | 4 |
| 7 | CAD (LAB) | 23 | 47 | 70 | 2 | 7 | AIRCRAFT MATERIALS & PRODUCTION (LAB) | 25 | 50 | 75 | 2 |
| 8 | MOS & MOF LAB | 24 | 48 | 72 | 2 | 8 | ELECTRICAL & ELECTRONICS ENGG. (LAB) | 23 | 48 | 71 | 2 |
| | I SEMESTER | | | III YEAR | | | II SEMESTER | | | | |
| 1 | MANAGEMENT SCIENCE | 17 | 80 | 97 | 4 | 1 | FLIGHT MECHANICS-II | 17 | 49 | 66 | 4 |
| 2 | FLIGHT MECHANICS-I | 15 | 33 | 48* | 4 | 2 | AEROSPACE VEHICLE STRUCTURES-II | 14 | 69 | 83 | 4 |
| 3 | AERODYNAMICS-II | 13 | 61 | 74 | 4 | 3 | AEROSPACE PROPULSION-II | 17 | 52 | 69 | 4 |
| 4 | AEROSPACE VEHICLE STRUCTURES-I | 16 | 41 | 57 | 4 | 4 | FLIGHT VEHICLE DESIGN | 12 | 61 | 73 | 4 |
| 5 | AEROSPACE PROPULSION-I | 13 | 52 | 65 | 4 | 5 | FINITE ELEMENT AND MODELING METHODS | 17 | 48 | 65 | 4 |
| 6 | CONTROL SYSTEMS | 17 | 49 | 66 | 4 | 6 | INTRODUCTION TO SPACE TECHNOLOGY | 13 | 54 | 67 | 4 |
| 7 | ADVANCED ENGLISH COMMUNICATION SKILLS LAB | 25 | 49 | 74 | 2 | 7 | AEROSPACE STRUCTURES (LAB) | 25 | 49 | 74 | 2 |
| 8 | AERODYNAMICS AND PROPULSION LAB | 25 | 46 | 71 | 2 | 8 | FLIGHT VEHICLE DESIGN (LAB) | 24 | 49 | 73 | 2 |
| | I SEMESTER | | | IV YEAR | | | II SEMESTER | | | | |
| 1 | VIBRATIONS AND STRUCTURAL DYNAMICS | 18 | 37 | 55 | 4 | 1 | AIRCRAFT SYSTEMS AND INSTRUMENTATION | 19 | 65 | 84 | 4 |
| 2 | COMPUTATIONAL AERO DYNAMICS | 13 | 61 | 74 | 4 | 2 | HYPERSONIC AERODYNAMICS | 16 | 62 | 78 | 4 |
| 3 | STRUCTURAL ANALYSIS AND DETAILED DESIGN | 13 | 56 | 69 | 4 | 3 | AIRCRAFT MAINTENANCE MANAGEMENT | 18 | 61 | 79 | 4 |
| 4 | AVIONICS | 17 | 57 | 74 | 4 | 4 | INDUSTRY ORIENTED MINI PROJECT | - | 49 | 49 | 2 |
| 5 | AIRPORT MANAGEMENT | 18 | 54 | 72 | 4 | 5 | SEMINAR | 48 | - | 48 | 2 |
| 6 | ROCKETS AND MISSILES | 17 | 54 | 71 | 4 | 6 | PROJECT WORK | 39 | 159 | 198 | 10 |
| 7 | COMPUTATIONAL STRUCTURAL & AERODYNAMICS (LAB) | 24 | 49 | 73 | 2 | 7 | COMPREHENSIVE VIVA | - | 96 | 96 | 2 |
| 8 | STRUCTURAL ANALYSIS AND DETAILED DESIGN (LAB) | 22 | 48 | 70 | 2 | | (# Project Internal 40, External 160) | | | | |

Number of Credits registered for: 224 Aggregate Marks Secured for [illegible] 216

Aggregate Marks Secured: 4190 OUT OF 5275 (79.43%)

Date of Issue: June 15, 2012

[illegible]

A indicates "ABSENT"

(*Courses registered but not counted for calculation of aggregate)

CONTROLLER OF EXAMINATIONS

At last verifiers can view certificates digitally. This can eradicate the fake certificates, proxy.

## 5.CONCLUSION

Digital Certificate Management system aspires to create the vision of Advanced Scholarly Certificates for each Indian a reality. This touches the lives of Indian youth and engages them with Computerized, Online, Trusted, Unquestionable Certificates which are open in a secure way at all times. DCM guarantees to do absent with troubles / wasteful aspects of collecting, keeping up, and displaying physical paper certificates. DCM may be a total framework for Issuing Online Certificates to Well Recognized and Enrolled Understudies. DCM coordinating specifically with Sheets / Colleges who issue Certificates and subsequently guarantees Genuineness of Certificate Records.

- The Scholastic Educate hold up the points of interest of the scholastic records within the depository system;

- The understudies get to their certificate records in their accounts which are kept up within the store framework;

- The confirmation clients I.e. banks, bosses, scholarly teach get to the store

## 6.FUTURE ENHANCEMENT

Digital signatures can be Wave of the Longer term Some person once told me that the tin can was designed a few a long time some time recently the can opener. I do not know on the off chance that that's genuine, but much obliged to the quick pace of innovative advancement, we in some cases discover ourselves looking at a superb, air proof, tin-can arrangement to a issue as it were to realize afterward we ignored to design a can opener. These days, advanced signature innovation is the tin can that will make electronic records reasonable. All we require presently are the laws, arrangements and trade hones that will let us get to the soup inside. Fortunately, Washington, Massachusetts, Texas and the Social Security and Common Administrations organizations, to title but a number, of are working difficult to design a "can opener." The signature has been the establishment of trade and government exchanges for thousands of a long time. Be that as it may, the apparatuses of government and commerce are changing. Bits and bytes are supplanting write and material. Data is being made, changed and exchanged more regularly and more quickly than ever some time recently. Cutting edge communication apparatuses have made nearly boundless openings to progress data stream and forms, but they have not dispensed with the lawful, cultural and practical require for unmistakable and enduring representation of commitment. Computerized marks are today's reply to that age-old require. Advanced marks will someday deliver us the capacity to routinely execute official trade between government and the open over computer systems. Shockingly, the political, legitimate and specialized framework fundamental to bolster far reaching execution of such an open public-key framework (PKI) appears to be a few a long time .

## 7.REFERENCE

1.Barry Burd, “Java Server Pages”, 1st Ed, IDG Books India(p) Ltd, pg 31-104, 237-298, 305-355.

2.Richard Fairley, “Software Engineering Concepts”, 7th Ed., Tata McGraw Hill, pg282-303.

3.H.M. Deitel & P.J. Deitel, “Java How to program”, 6th Ed., PEARSON Education, pg. 1346-1392.

4.Kevin Loney, George Koch, “ORACLE The Complete Reference”, Tata McGraw Hill, pg. 41-69 & 165-190.

5.James Goodwill, "Developing Java Servlets", SAMS Tech media, pg.145-199, 253- 269 & 281-299.

6.Grady Booch, James Ram baugh, Ivar Jacobson, "The Unified Modelling Language User Guide", 12th Ed, Pearson Education, pg. 219-229,233-239,205-215 & 243-255.

7.Raghu Rama Krishnan, Johannes Gehrke, "Database Management Systems", 2nd Ed. Mc Graw Hill, 24-45 & 119-150.

8.Roger Pressman, Software Engineering-A practitioners Approach", 5th Ed., Mc Graw Hill, pg. 36-38,485-494.

9.Simon Roberts, Philip Heller, Michael Ernest, "Java 2 Certification Study", BPB Publications, pg. 509-536.

10.Korth F Henry, "Database System Concepts", 4th Ed., Mc Graw Hill, pg. 27-62, 135- 168 & 225-238.