Idea/Approach Details

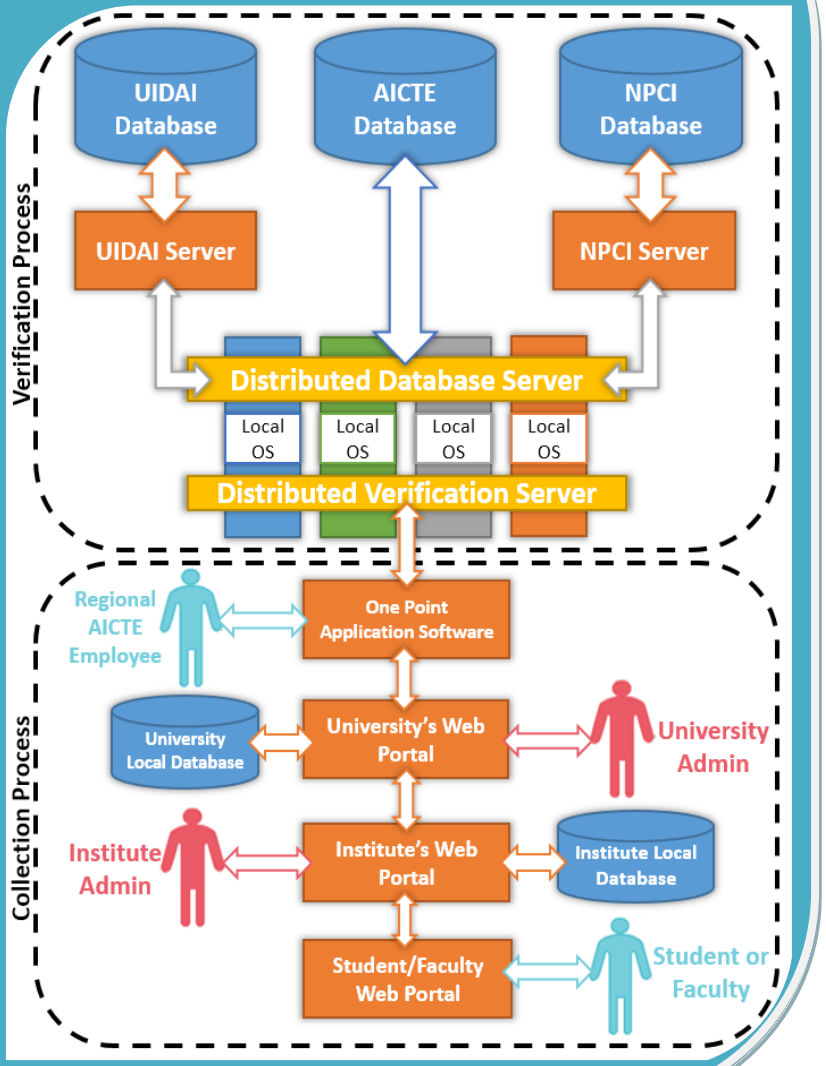
Ministry Category: AICTE
Problem Statement: One Point Verification System Through Functional Application Software
Team Leader Name: Aditya Bhardwaj

Problem Code: #AIC3
Current AICTE Application No: 1-3329193700

- **IDEA:** Our core idea is to provide a common web portal to the Universities/Institutes for collecting the data from Students/Faculties/Staff and processing the collected data at the Distributed Servers for verification with UIDAI and NPCI.

- **APPROACH**: The above problem can easily be classified into 2 broad processes:

1. **Verification of Details**
   a. Complete but unverified records present in AICTE database would be processed for authentication with UIDAI and NPCI on the Distributed Verification Servers.
   b. Records will be first authenticated with UIDAI using Aadhaar Authentication API which submits the details to the CIDR for verification and generates a response of either "yes" or "no".
   c. Only after a successful authentication, NPCI Mapper or Aadhaar Payment Bridge System(APBS) is requested with Aadhaar Number. NPCI responds with the bank details linked with the Aadhaar Number which our server matches with the collected details.
   d. The status of verification is updated to the AICTE Database against each record.
2. **Collection of Missing Details from Students/Faculties/Staff for further verification.**
   a. For this purpose, a common web portal will be designed which would serve as a registration desk and would assist in collection of details in a uniform and structured pattern.
   b. Each individual would be registered and will be provided with a login ID and password.
   c. Each individual's details would be first approved with local records by the admin of higher body i.e. Institute, University and Regional AICTE Offices, before being sent to AICTE's servers.
   d. After the approval, these records would be moved into "Complete but unverified" category and will be processed accordingly.
3. **Intimation to individuals:** All the individuals would be updated with latest status via E-Mail and SMS, and could also view their latest status at OPV's Login Portal.
4. **Direct link between Student and AICTE:** The Aadhaar number and the OPV's web portal would serve as a direct link between the Student and AICTE and can be used for additional purposes.
5. **Provision of fingerprint scanning(Optional):** We can also introduce automated data collection by using Biometrics/OTP for authorizing the e-KYC provision of UIDAI to fetch Personal and Bank Details from UIDAI.
6. **Secure Data Transmission:** Use of advanced encryption techniques such as SSL or TLS will ensure secure transmission of confidential data.



Technology Stack & Dependencies

- **TECHNOLOGY STACK**:
  - **Backend: (Server and Clients Handling)**
    - Java Servlet Programming (Application Server)
    - Apache Tomcat Server (Client handling)
    - Network-Client Communication (Http Get and Post)
  - **Frontend: (Software and Web Interface)**
    - Java Swing (Software GUI)
    - HTML (Web GUI)
    - CSS (Web GUI Styling)
    - AngularJS (A JavaScript Framework)
    - Bootstrap (Web Responsiveness)

- **DEPENDENCIES**:
  - UIDAI Database (For Personal Details): Database must be updated with latest information.
  - NPCI Database (For Bank Details):Database must be updated with latest information. Also bank account must be Aadhaar seeded.
  - AICTE Database: Student/Faculty must have registered unique identification number such as enrolment number or Faculty Id in AICTE Database updated with latest information.
  - Good Connectivity (Internet Connection)
  - Server Hardware capacity: Hardware used for server must be reliable and must have powerful processing capacity with high multi-threading support.
- **SHOW STOPPERS**:
  - Poor Internet Connectivity
  - Unavailability of Database Server (Servers maybe offline)
  - Hardware failure
  - Denial of Service by server due to overcrowding of clients

Use Case Diagram