DBMS Minor Project

AADHAAR CARD :

" vision for new India "

— Bhaskar
180001012
— Rishabh Kumar Yadav
180003044

INTRODUCTION :-

In the modern time, the age of computers, an era in which INFORMATION is everything, it is the need of the hour to make the access of information faster, more efficient and more transparent. This can be done by the introduction of a mastercard which links all the information of a person from various field he is linked with. This process can be automated so that the society runs hand in hand with the government and take the nation's growth at a higher level. The automation of the process also ensures that all the information attributed to a person is stored collectively and is connected.

VISION :

The Aadhaar Card will be a unique id of a person in the nation given by an Aadhaar number. The Aadhaar card will be a link or authorising card for various other departments.

for example, Aadhar card will link PAN Card, Passport, voter-id card, Driving Licence, DOB certificate, Work ID, etc.

WORKING :

The Aadhaar Card will generate a unique ID, i.e., the Aadhaar number, which will allow to link various entities in an authenticated way so that the sharing of information among various departments can take place easily. Some of the departments are listed below:

PAN Card, Passport, Driving License, Voter ID Card, Gun License, Digilocker

from here we can see the linking b/w various departments accessible to the government & the individual.

UID database would be used by making a query. The query will provide the UID Numbes along with one of the parameters such as name. The answer returned will be either 'True' or 'False'. The users will mostly be service providers who check the ID of a prospective client. Return of 'False' information by database or it's inability to match of a genuine query could be security threats discussed later.

PROCESSES INVOLVED :

There are various processes involved for which various software applications are being used. which are discussed later in detail.

But more basically we are concerned with the maintainance of database & basic queries will be :

(i) creation of new cards.

(ii) updating the information

(iii) Seizing the cards of non-existing people and updating their death record & card seize record.

The advanced queries for smooth functioning of the database requires proper

(i) Authentication

(ii) fraud detection

(iii) Administration

and (iv) logistic support.

SCOPE :

1. The prevention of illegal voter IDs can be enforced. This ensures that one person can have a maximum of one voter ID.

2. Uniqueness of Ration Card is ensured. Thus, people cannot avail ration facilities in a quantity more than prescribed by the government.

3. Records of families are interrelated. This keeps a check on the sum total of the assets owned by an individual or his family. It thus prevents the faking of Income Tax Returns.

4. A young holder of Aadhaar Card, if gets lost, can be identified. The finger print can be used to retrieve his data and get him back to home.

5. Digilocker is an online service which people can avail by signing in using their Aadhaar Number. It stores the important documents of people.

6. With the introduction of Aadhaar, the issuing of passport will become faster.

7. Pensioners will lead a digital Aadhaar based life.

8. Whitening of black money in stock markets will be prevented.

SOFTWARE APPLICATIONS USED:

Aadhaar database (CIDR (Central ID Repository)) is hosted on a central system powered by data centers. This data is used to serve Aadhaar project's core objectives as mentioned.

(1) ENROLMENT APPLICATION:

Used for recieving new client enrolment requests and capturing new data. After verifying the uniqueness of the request, the registars enroll the data that is received in magnetic media from various logistic providers. This data is then uploaded to Aadhaar database post-validation. The Registrars include ministries & departments of state & central govt., banks & other financial institutions, telephone companies etc. Once this is done the Aadhaar number is generated for the request.

(2) AUTHENTICATION APPLICATION

Conduct online authentication of identity (demographic & biometric info.) done by querying the Aadhaar database that responds to such queries in the form of Valid/Invalid type of response.

(3) FRAUD DETECTION APPLICATION :-

detects identity fraud by catching fraud scenarios.

for eg: registration for non-existent applicants mis-representation of information, multiple registration attempts by same applicant, user impersonation etc.

④ ADMINISTRATIVE APPLICATION :

It provides user management, role-based access control, automation & status reporting.

⑤ ANALYTICS & REPORTING APPLICATION :

It provides enrolment & authentication statistics for both public & patners

⑥ INFORMATION PORTAL :

It provides administrative access for internal users, patners & general information/reports/ grievance requests details to public.

⑦ CONTACT CENTER INTERFACE APPLICATION :

It will provide query & status updates.

⑧ LOGISTICS INTERFACE APPLICATION :

It interfaces with the logistics provider for letter printing & delivery mangement.

I INFORMATION SECURITY RISKS INVOLVED

(i) Unauthorized access to Aadhaar project database could have disastrous effects.

(ii) Ownership of PKI (Public Key Infrastructure) implementation lies with the registrars. As a result, there is a risk of use of broken encryption algorithms by registrars at the time of recieving updates from CIDR thereby compromising data confidentiality.

(iii) Backup mechanism & Recovery time objectives of aadhaar project database in case of natural/technical failure may prove a challenge considering the scale of the project.

(iv) There may also be operational challanges. for instance, updating of current demographic information, change of residence or martial status by existing aadhaar holders may be challenging.

SECURITY MEASURES :

The UID is much more secure than having a physical card. One can produce duplicate copies of the physical card, can steal it, etc. but stealing someone's biometric identity is not an easy task.

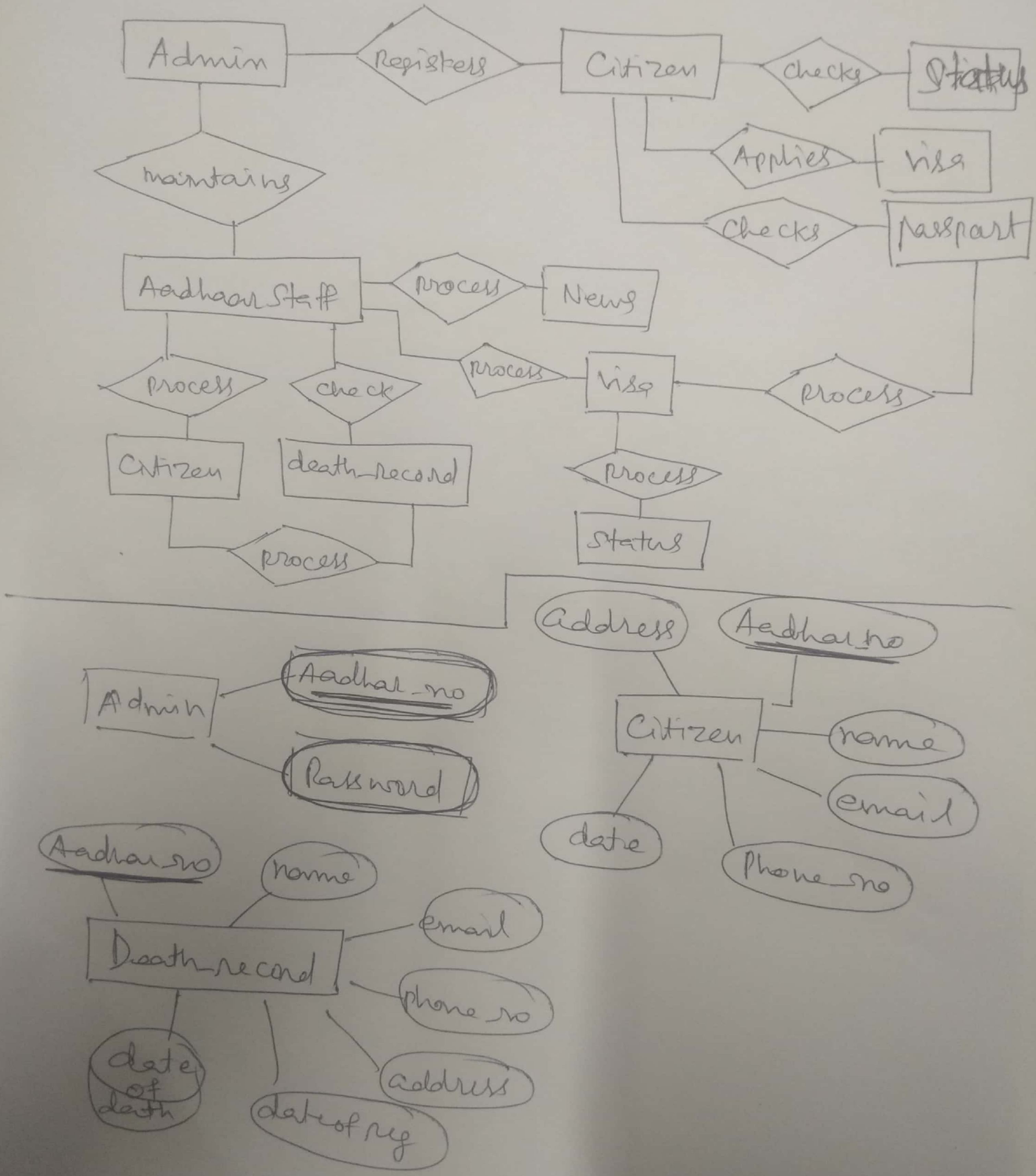
1. Securing the central database : The major threats to UID centralized database are unauthorized access to UIDAI servers, organized attack from cyber warriors or cyber terrorists and stealing and leaking of sensitive information. Strong role-based access control, firewall, intrusion detection system, manpower training and background check are critical measures to ensure security of UID centralised database.

2. Security during transmission : The UID authentication is biometric. It is based on the match between a fresh scan and a previously stored image. During transmission, the data may be manipulated by hacking the servers. It may affect the matching process and a genuine person may be denied services.

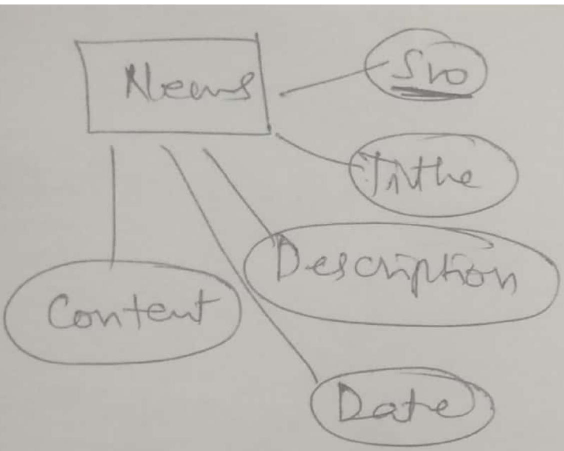
An application will be developed which transmits the data in encrypted form so that transmission security can be managed.

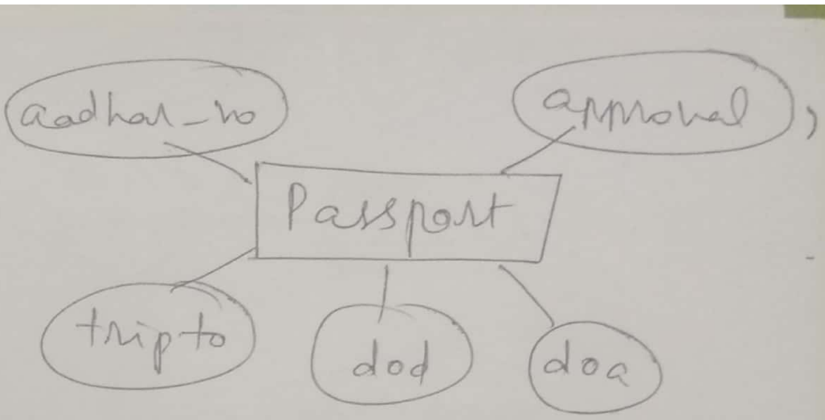
3. At the time of authentication, only the UID number is verified for ensuring the data privacy.

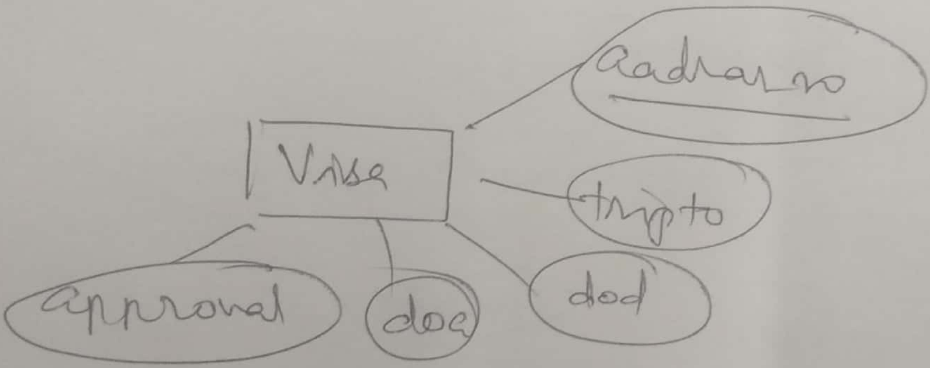
tus)

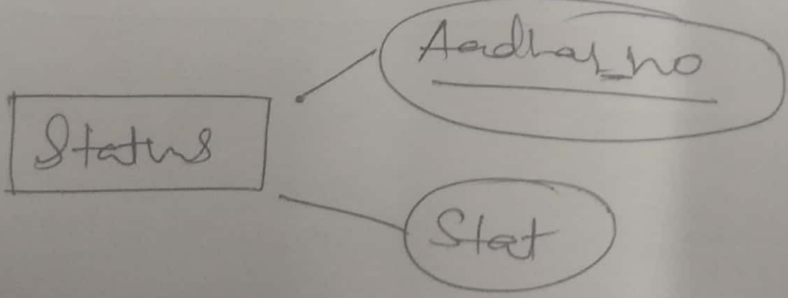

Admin
Registers
Citizen
Checks
~~Status~~
Applies
visa
Checks
passport
maintains
Aadhaar Staff
process
News
process
check
process
visa
process
Citizen
death_record
process
Status
process
Admin
Aadhar_no
Password
Address
Aadhar_no
Citizen
name
email
date
Phone_no
Aadhar_no
name
email
Death_record
phone_no
date of death
date of reg
address

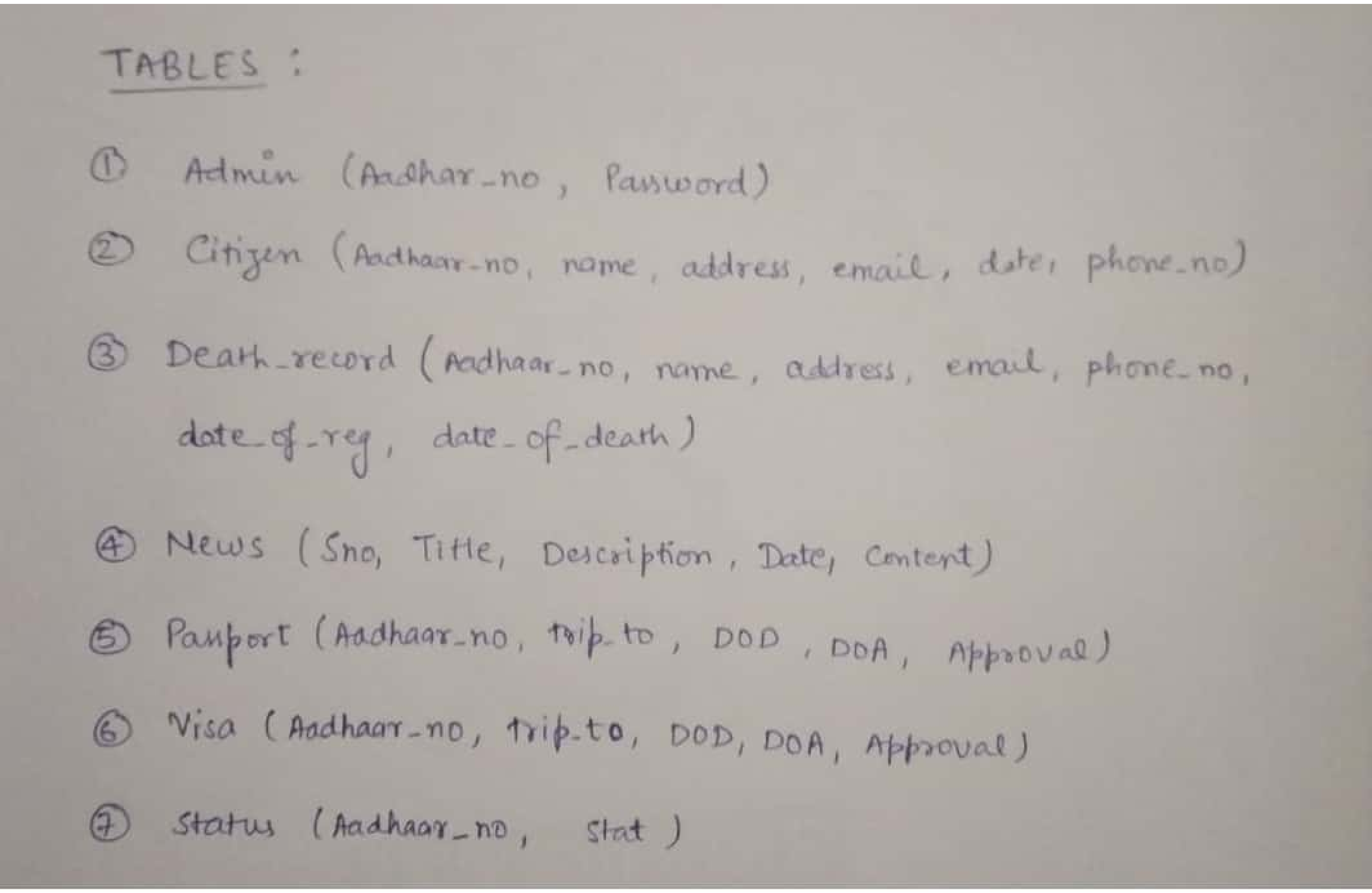
2019.11.15 17:


News
Sno
Title
Description
Content
Date


aadhar_no
approval
Passport
tripto
dod
doa


aadhar_no
Visa
tripto
approval
doa
dod


Aadhar_no
Status
Stat



TABLES :

1. Admin (Aadhar_no , Password)
2. Citizen (Aadhaar-no, name, address, email, date, phone_no)
3. Death_record (Aadhaar_no, name, address, email, phone_no, date_of_reg, date_of_death)
4. News (Sno, Title, Description, Date, Content)
5. Passport (Aadhaar_no, trip_to, DOD, DOA, Approval)
6. Visa (Aadhaar_no, trip_to, DOD, DOA, Approval)
7. Status (Aadhaar_no, Stat)