|  |  |
| --- | --- |
| **PR** | **Private Key** |
| **PU** | **Public Key** |
| **SID** | **System ID** |
| **UID** | **Unique Identification Number** |
| **DoB** | **Date of Birth** |
| **P-OTP** | **Password-One Time Password** |
| **QR-SID** | **Quick Response Code-System ID** |
| **QR-PU** | **Quick Response Code-Public Key** |
| **E(Message , Key)** | **Encrypt message using key** |
| **D(Cipher , Key)** | **Decrypt message using key** |
| **H(A,B)** | **Hash of A and B** |
| **DOC1** | **Original Document/Report** |
| **C-DOC1** | **DOC1 Encrypted by Patient** |
| **C-DOC2** | **DOC1 Encrypted by Doctor** |

**BLOCKCHAIN MEDICAL SYSTEM**

**LEGEND**

**DB**

**5. Success. Store SID, Mobile, Medical History, H(SID, Password)**

**A. Authorize UID, Mobile, Demographic details using Aadhaar API’s**

**C. Validation Compare Received & Generated P-OTP**

**B. SID & P-OTP Generation SID=H(UID,Demographic) Generate Random P-OTP**

**5. Success. SID**

**2. UID, Demographics, Mobile**

**3. SID, P-OTP**

**D. Generate QR-SID Cipher=E(SID,Password)QR=Encode(Cipher)**

**1. UID, Demographics, Mobile, Medical History**

**6. QR-SID to be stored in App**

**3. P-OTP**

**4. Received P-OTP, Password**

**PATIENT**

**E. Generate Public & Private Keys on user Device using SID and DoB**

**7. QR-SID, Password, DoB**

**7. QR-SID, Password,**

**CLINIC**

**8. PR, QR-PU**

**REGISTER PATIENT**

**A. Authorization**

Patient submits his Aadhaar Card, Mobile, Demographic & Medical history.

Details are validated using Aadhaar APIs

Patient Details are forwarded to SID & P-OTP Generation

**B. SID & P-OTP Generation**

Generates SID as SID = H(UID, Demographic)

Generates Random P-OTP and sends it to Patient’s Device

SID and P-OTP are forwarded to Validation

**C. Validation**

Compares received & generated P-OTP

Accepts Password from Patient

If Validation is Successful then SID, Mobile, Medical History, H(SID, Password) are stored in the DB and SID is forwarded to Generate QR-SID

**D. Generate QR-SID**

QR-SID is generated as Cipher = E(SID,Password) and QR = Encode(Cipher)

QR-SID is forwarded & stored on Patient’s Device

**E. Generate Public & Private Keys on Patient’s Device**

Patient’s generated QR-SID, Password and Date of Birth (DoB) are taken as input

SID = Decode(QR-SID, Password)

SID and DoB is used to generate and store Public & Private Keys on Patient’s Device

**C. DOC1=D(C-DOC1, PR1) C-DOC2=E(DOC1,PU2) on Patient Device**

**DB**

**11. C-DOC1, PR1, PU2**

**7. SID, C-DOC1=E(DOC1, PU1)**

**8. Request C-DOC1**

**12. C-DOC2**

**6. Generate DOC1**

**9. PU1**

**B. SID=D(Cipher,Password)**

**A. Cipher=Decode(QR-SID)**

**2. QR-SID**

**4. Password**

**CLINIC**

**1. QR-PU1, QR-SID**

**10. PU2**

**PATIENT PR1, QR-PU1, QR-SID**

**13. C-DOC2**

**DOCTOR PR2, QR-PU2**

**SUCCESS/FAILURE Notification**

**15. DOC1**

**14. C-DOC2, PR2**

**3. Cipher**

**DB**

**5. SID, H(SID,Password)**

**D. DOC1=D(C-DOC2, PR2) on Doctor Device**

**MEDICAL CHECK-UP**

1. Patient allows Clinic to Scan his QR-PU1 and QR-SID

2. Forward QR-SID to Step A

**A. Decode QR-SID to get Cipher**

3. Forward Cipher to Step B

4. Patient submits Password to Step B

**B. Cipher is decrypted using Password to produce SID**

5. SID and H(SID, Password) entry is made in the DB

**SUCCESS/FALIURE Status is sent to the Client**

6. Clinic generates Patient Report named DOC1

7. Clinic encrypts DOC1 using PU1 as C-DOC1 & makes an entry in the DB of SID, C-DOC1

8. Patient requests C-DOC1 from DB

**Patient goes to a Doctor for a Check-Up**

9. Patient lets Doctor to scan his QR-PU1 to obtain PU1

10. Doctor lets Patient to scan his QR-PU2 to obtain PU2

11. Patient forwards C-DOC1, PR1 and PU2 to Step C.

**C. DOC1 is obtained by D(C-DOC1, PR1) and C-DOC2 is obtained by E(DOC1,PU2). This is done on the Patient’s Device**

12. Step C stores C-DOC2 on Patient’s Device

13. Patient forwards C-DOC2 to Doctor’s Device

14. Doctor forwards C-DOC2 and PR2 to Step D.

**D. DOC1 is obtained by D(C-DOC2, PR2). This is done on the Doctor’s Device**

15. Step D stores C-DOC1 on Doctor’s Device

**5. Success SID**

**3. SID, P-OTP**

**2. UID, Demographic**

A. Authorize UID, Mobile, Demographic using Aadhaar

D. Generate QR Code

Cipher=E(SID, New Password)

QR=Encode(Cipher)

B. Re Generate

SID=H(UID, Demographic)

Generate Random P-OTP

C. Validation

Compare Received & Generated

P-OTP

DB

**5.**

|  |  |  |  |
| --- | --- | --- | --- |
| **SID**  **3. P-OTP**  **4. Received P-OTP, New Password** | **Mobile** | **Medical History** | **H(SID, New Password)** |
|  |  |  |  |



**FORGOT PASSWORD**

**6. QR to be stored in App**

1. **Mobile , UID ,Demographic Medical History**

**A. Authorization**

Patient submits his Aadhaar Card, Mobile, Demographic, Medical history.

Details are validated using Aadhaar APIs

Patient Details are forwarded to SID & P-OTP Generation

**B. Re-Generate SID & P-OTP Generation**

Re-Generates SID as SID = H(UID, Demographic)

Generates Random P-OTP and sends it to Patient’s Device

SID and P-OTP are forwarded to Validation

**C. Validation**

Compares received & generated P-OTP

Accepts New Password from Patient

If Validation is Successful then SID, H(SID, New Password) are updated in the DB and SID is forwarded to Generate QR-SID

**D. Generate QR-SID**

QR-SID is regenerated as Cipher = E(SID, New Password) and QR = Encode(Cipher)

QR-SID is forwarded & stored on Patient’s Device