|  |  |  |
| --- | --- | --- |
| **Operations** | **Algorithm** | **Database** |
| START |  |  |
| Registration | Password and Username encryption Using MD5  OTP Authentication  Database data;  if(mbl\_number==data.mbl\_number) | Storing of User Details |
| Login | Password and Username decryption Using MD5  Database data;  if(username.validate(data.username)  &&password.validate(data.password)) | Checking credentials |
| Dashboard |  |  |
| Account Summary | Fetching of account details from database | Responding |
| Check Balance | OTP Authentication |  |
| Send Money | OTP Authentication | Updating Balance |
| OTP Verification | Sms sms;  if(otp==sms.otp) |  |

**OTP AUTHENTICATION:**

|  |  |
| --- | --- |
| **Input** | **Generation** |
| 0123456789 | Random r=new Random(); |

**Password Encryption and Decryption:**

|  |  |
| --- | --- |
| **Input** | **Generation** |
| password | **\*PBE:** Using this a AES or a DES encryption key is derived and encrypted.  PBEKeySpec pbeKeySpec = new PBEKeySpec(password.toCharArray());  **\*SecretKeyFactory:** This class is used for generating secret symmetric keys. In other words, it generates a SecretKey object from the input key specification.  SecretKeyFactory secretKeyFactory = SecretKeyFactory.getInstance("**PBEWithMD5AndTripleDES**");  **\*Cipher:** The term Cipher is standard term for an encryption algorithm in the world of cryptography.  Cipher.getInstance("PBEWithMD5AndTripleDES");  cipher.init(Cipher.**ENCRYPT\_MODE**, secretKey, pbeParameterSpec);  cipher.init(Cipher.**DECRYPT\_MODE**,secretKey, pbeParameterSpec);  **\*Salt:** a salt is [random](https://en.wikipedia.org/wiki/Random_Number_Generator) data that is used as an additional input to a [one-way function](https://en.wikipedia.org/wiki/One-way_function) that "[hashes](https://en.wikipedia.org/wiki/Cryptographic_hash_function)" [data](https://en.wikipedia.org/wiki/Data_(computing)), a [password](https://en.wikipedia.org/wiki/Password) or [passphrase](https://en.wikipedia.org/wiki/Passphrase). Salts are used to safeguard passwords in storage. |