|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **id** | **user\_id** | **token\_hash** | **expiration** | **created\_at** | **last\_used** |
|  |  |  |  |  |  |
| 1 | 101 | 5e884898da28047151d0e56f8dc629277... | 2024-12-01 10:00:00 | 2024-11-25 10:00:00 | 2024-11-25 12:00:00 |
| 2 | 102 | 2b9e64d8a813a0ecba3459a53a75d2f8c... | 2024-12-02 11:00:00 | 2024-11-25 11:00:00 | 2024-11-25 13:00:00 |
| 3 | 103 | a3f390d88e4c41f2747bfa2f1b5f87dbd... | 2024-12-03 12:00:00 | 2024-11-25 12:00:00 | NULL |
| 4 | 104 | 98c55da5dc06709e6a4777ad2d6c1234f... | 2024-12-04 13:00:00 | 2024-11-25 13:00:00 | 2024-11-25 14:00:00 |
| 5 | 105 | d2d0714f014a9784047eaeccf956520045... | 2024-12-05 14:00:00 | 2024-11-25 14:00:00 | NULL |

**Database task:**

* Implement the token by generating the random strings using UUIDSs or JWTs with strong signing keys
* Store hashed tokens in the database with the attributes such as: User ID, token\_hash, expiration, created\_at and last\_used.
* The tokens can be validated by checking the database for its validity and expiration
* Also, a rate limit can be added to make sure the users’s request don’t exceed at least 5.