# Team Name: Digineers

# Track: Identification and Verification

# Team Members

|  |  |
| --- | --- |
| Name | Key skills |
| Sachin Patel | Noise filtration and digital data analysis. (Eager to lay hands on Blockchain & Cognitive APIs) |
| Dimple Mehta | User experience and User Interface designs. (Eager to lay hands on Blockchain & Cognitive APIs) |
| Jaiveer Shringi | Novice in these technologies. (Eager to lay hands on Blockchain & Cognitive APIs) |

# Identified Use Case(s)

*Identification and Verification.*

**Problem**: How can we easily capture the customer’s digital identity?

* Digital identity team has considered:
  + Biometric (Finger Print)
  + VoicePattern *OR* Face
* Registration of a user through an app interface to be used as a means to capture Digital identity.
  + Capture and Validate/Verify Biometric (Finger Print) information using Operating System API’s.
  + Capture and Validate/Verify user Voice Print (including name and eMail) information using Operating System API’s.
  + Register user based on the email information, sending a verification link and recording a password for alternative access.
* *Pain area/problems in implementing each use case:*
  + Capture and Validate/Verify Biometric (Finger Print) information using Operating System API’s.

Hardware dependent and tied to the device and thus to API’s available.

* + Capture and Validate/Verify user Voice Print (including name and eMail) information using Operating System API’s followed by:

*Voice Activity detection*

*Extracting features*

*Classifying and Mapping those features to Verify*

* *Narrate use case describing what and how you intend to demonstrate*

A new user when trying to register in the Application is requested for the following information in order:

* Use of Fingerprint stored on the device
* Voice print narrating name and eMail address

This latter is first filtered for any/all noise, eMail information extracted & used to post a verification link which also serves to record password for alternative access.

This verification link stays active for 15 minutes post which the non-verified attribute data gets cleared from the storage.

If verified, the data is passed to a Web API first communicating with Cognitive services or Open Blockchain networks to manage voice print identity and second logging the registration into the existing user base.

If the user then returns to login, following information is requested:

* Use of Fingerprint stored on the device & Voice print narrating name and eMail address

OR

* eMail & Password.

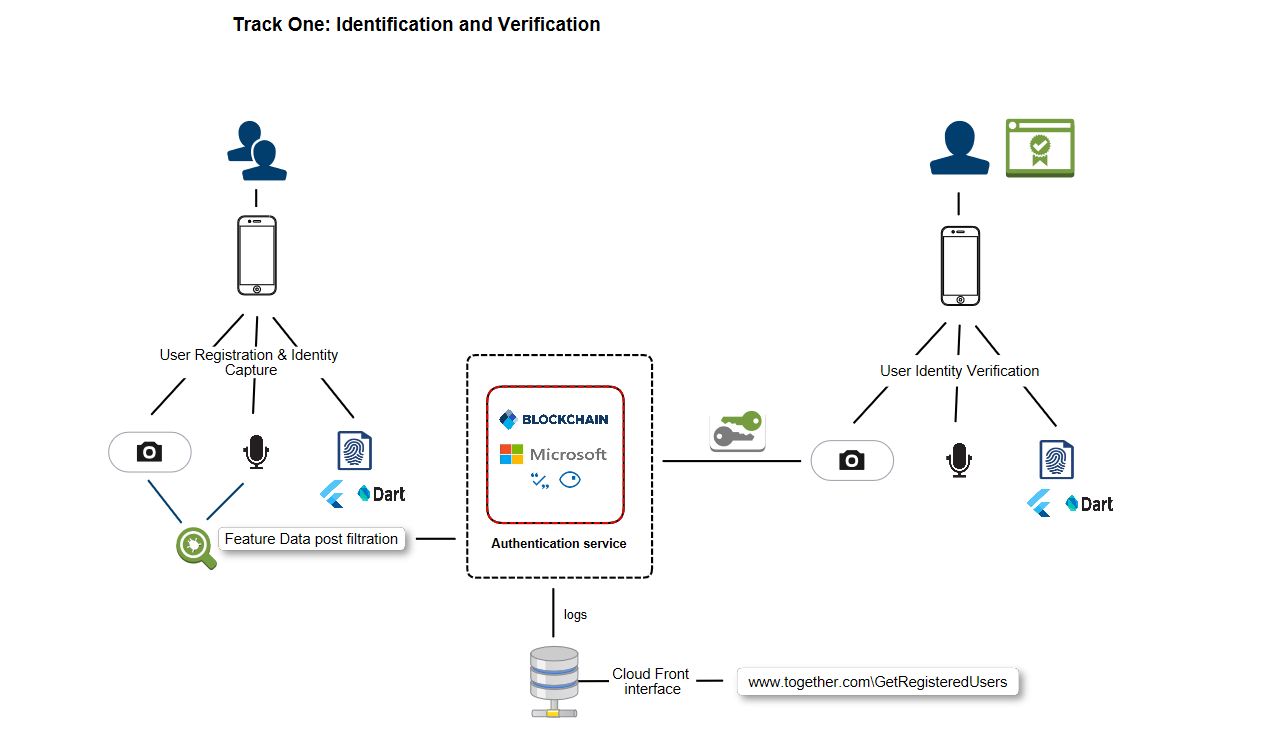
On providing relevant information in either case user should be allowed to login, Otherwise prompted an access failure message.

# High level solution

Solution support platform: Mobile Application

Assumptions:

* Robust and uninterrupted internet connectivity.
* Decent device configuration, hardware includes fingerprint scanner and/or good microphone.



# Support required

*Call out for support that team may require for implementing solution. Support could be in terms of computing facilities, connectivity, any software/hardware/services/APIs etc.*

Team would appreciate the following:

Hardware:

* A good connection to the internet to learn anywhere anytime as well as download bigger volumes of data which would be required for various AI frameworks.
* Provisions to carry individual Laptops or availability of provisional laptop/machine from Mastek with decent configuration.

Software/Services:

* Guidance on Flutter with DART APIs for Identity capture and Management.
* Guidance on use of Microsoft cognitive services (Vision/Face API, Speaker recognition API etc.)
* Guidance on use of Ethereum open blockchain network and its robustness WRT identity management and data immutability.

To offer a simple, seamless yet secure mode of user identification. This is achieved by extending the registration process through a handheld mobile app using three essential and unique pieces of information to establish identity:

* Something you are (Face)
* Something you know (Voice passphrase)
* Something you have (Finger Print)

Recognition is then divided in two phases:

Registration\Enrolment Identification\Verification (tightly coupled with a pass phrase in case of voice)

**Face Recognition:**

Since face is the most easily accessible and widely acceptable form of identity, facial recognition has been considered as the prime use case. This as mentioned is achieved in two steps:

**Registration\Enrolment**: Capturing live video though a mobile app using device’s front camera which is then sampled and random frames passed on for registering the user. This in turn calls Microsoft Azure Face API, enrolling the user to a predefined group followed by training to store facial features.

**Identification\Verification**: Requesting a live video though the same interface which is then sampled and random frames passed on for comparison with the enrolled user base. This in turn calls Microsoft Azure Face API, checking whether each Image returns the same user information and thus verifying user identity.

**Limitations:** Size of image not more than 4 MB, Requires a Azure licence, Limited to identifying faces without any accessories covering the essential facial features.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Identifiers** | **Registration\Enrolment** | **Identification\Verification** | **USP’s** | **Limitations** |
| **Face Recognition** | 1) Capturing live video though a mobile app using device’s front camera.  2) This is then sampled and random frames passed on for registering the user.  This in turn calls Microsoft Azure Face API, enrolling the user to a predefined group followed by training to store facial features. | 1) Requesting a live video though the same interface.  2) This is then sampled and random frames passed on for comparison with the enrolled user base.  This in turn calls Microsoft Azure Face API, checking whether each Image returns the same user information and thus verifying user identity. | 1) Most easily accessible and widely acceptable form of identity.  2) Verified from a live video using random frames thus reducing chances of impersonation. | Size of image not more than 4 MB, Requires a Azure licence, Limited to identifying faces without any accessories covering the essential facial features |
| **Voice Print Recognition** | 1) Capturing live video though a mobile app with instructions to speak a phrase a fixed number of times.  2) This is then sampled and voice print passed on for registering the user.  This in turn calls Microsoft Azure Voice API, enrolling the user storing voice print features. | 1) Requesting a live video though the same interface with instructions to speak a phrase a fixed number of times.  2) This is then sampled and voice print passed on for comparison with the enrolled user base.  This in turn calls Microsoft Azure Voice API, checking whether voice print is enrolled and thus verifying user identity. |  |  |
| **Fingerprint Recognition** |  |  |  |  |