April 03, 2019

Adaptive Authentication using User's Uniqueness Quotient

Tulika Varma

Harippriya Sivapatham

Vijai Babu Madhavan

Adaptive Authentication using User's Uniqueness Quotient

Disclosed by: Tulika Verma, Haripriya M Sivapatham, Vijai Babu Madhavan

Abstract.

Identity of a person is multi-faceted. However the identities in IAM solutions typically include only the external facet like user's name, age, designation, role, high school name, etc. This information is used for securely identifying the user, by prompting security questions like "What is your mother's maiden name", "What is the name of your pet" etc. as part of an Authentication method or the reset password option. However in this age of information oversharing, such data could be easily harvested from social media to impersonate the user.

Hence we need a reliable user identification that is intuitive to the user but hard to spoof by others. The industry solution for this is to use biometrics. However biometric data is extremely sensitive as there is no way to reset if hacked. This invention addresses these shortcomings and provides a way to create a comprehensive user identity that is intuitive, cannot be stolen or impersonated and doesn't require any additional equipment.

In this invention we propose to:

1. Create a Uniqueness Quotient of the user.
A comprehensive new user identity called the "Uniqueness Quotient" or "Personal Identity" by considering various factors that make a person truly unique. The Uniqueness Quotient is built using two sets of data:

1) User's profile built based on his personality, values, experiences, and interests

2) User's significant other's profile from user's perspective - User's perception about personality, values, experiences, and interests of the significant other (spouse, parent, sibling, friend, etc.) in his life. As this connected profile is built from the user's perspective, it may not reflect the true nature of the other person. This distance from reality as perceived by the user adds to the robustness of the identity we are building.

The Uniqueness Quotient is created during user registration / on-boarding. User will answer a questionnaire which would be mostly pictorial in nature that would help build a high level profile. So, overall we propose to build two profiles, both from the user's perspective. In a true sense, a person is who he is and how he views his world. So, this "Uniqueness Quotient" represents the 360 degree profile of the user. NOTE: See Uniqueness Quotient section below for exact details of this.

2. Assess during authentication
On every subsequent login, user will be prompted with 3 add-on questions – one related to his profile, one related to his significant other's profile and one to help fine tune his profile.

3. Evaluate risk
User's responses are compared with the expected responses based on the profile. If it deviates beyond the acceptable level, then that user is flagged. Risk service can consume this as a risk factor and prompt user for step up authentication or deny access as needed. .

4. Continuously Learn and Fine tune Profile
The result of every login is fed back into the learning algorithm, to fine tune the profiling. This continuous learning helps build an accurate profile of the user.

In addition to assessing user's risk, these dynamic profile based questions could also be added to the

static Security Questions displayed during authentication or password reset, making them robust and hard to impersonate.

Problems Solved

1**) Robust and Intuitive User Identification –** The user identification currently is either limited to external attributes like name, age, role or is at the opposite end with extremely sensitive attributes like biometric or face ID. The Uniqueness ID for a user provides a middle ground by creating an identity mechanism that is dynamic, internal to the user and hence cannot be impersonated while being intuitive.
This can be used to assess the risk of authentication by the Risk service. Based on whether the user profile matches, appropriate risk score can be calculated and the user may be allowed or denied access or may be asked to go through step up authentication.

2) Dynamic user profile – After a user is on-boarded, the identifying information rarely changes. This static data creates the vulnerabilities like hacked accounts or known impersonators. Replacing this with a dynamic system that aligns with the changing nature of the user and prompting relevant questions suitable for the current state of the user makes this type of identification robust.

3) No static data to memorize – Users typically use the same set of data in almost all registrations. This is to make it easy for them to remember. However the Uniqueness Quotient here is calculated based on something that is intrinsic to the user. Hence the user doesn't have to memorize any answers. He simply has to answer true to his self and authentication is complete. This improves the ease of use over time.

Advantages

1) **Difficult to compromise**
This mechanism is cannot spoofed or impersonated even by people who know the user. This is based on dynamic state of thinking of the user. Two main factors that make it difficult to compromise are:

a) Profiling two people from user's perspective -There exist methods that evaluate a person in ISOLATION for his personality, interests etc and we can use them to authenticate a person. However, if someone knows a person very well, he can answer many of such questions correctly and can hack the real user account. However, this invention is difficult to compromise as it studies 2 people. It may be easy for a hacker who is close to the user to give correct answers about him, but it will be very difficult for him to give correct answers for the questions asked about the user's significant other. Also, as the significant other is profiled from the user's perspective, even someone who knows the user and the other person will not be able to provide the right answers.

b) Different questions each time at authentication - A particular trait can be identified through different types of questions. E.g if a person is an expert scuba diving, it's very likely that he has done it many times and he knows the nuances involved. Each time a different question can be presented to the user to identify that trait/skill during authentication. So, even if a hacker is able to get the answers of previous questions, he won't be able to answer the new questions correctly due to dynamic nature of these questions.

2) Additional risk factor that can be considered
Risk Service evaluates a variety of parameters to evaluate user's risk. Uniqueness ID can be one another factor that can be considered for risk evaluation. This enhances the Risk service and makes it more robust.

3) Robust than static security questions – (https://en.wikipedia.org/wiki/Security_question) Static security questions like "What is your mother's maiden name" are asked as part of Authentication using Security Questions and more commonly for the Forgot Password scenario. These static questions are typically easy to crack. This mechanism can be strengthened by adding dynamic profile based questions to the mix.

4) Ease of Use
User does not have to remember any questions or answers.

Description

Design

The following are the elements of the invention.

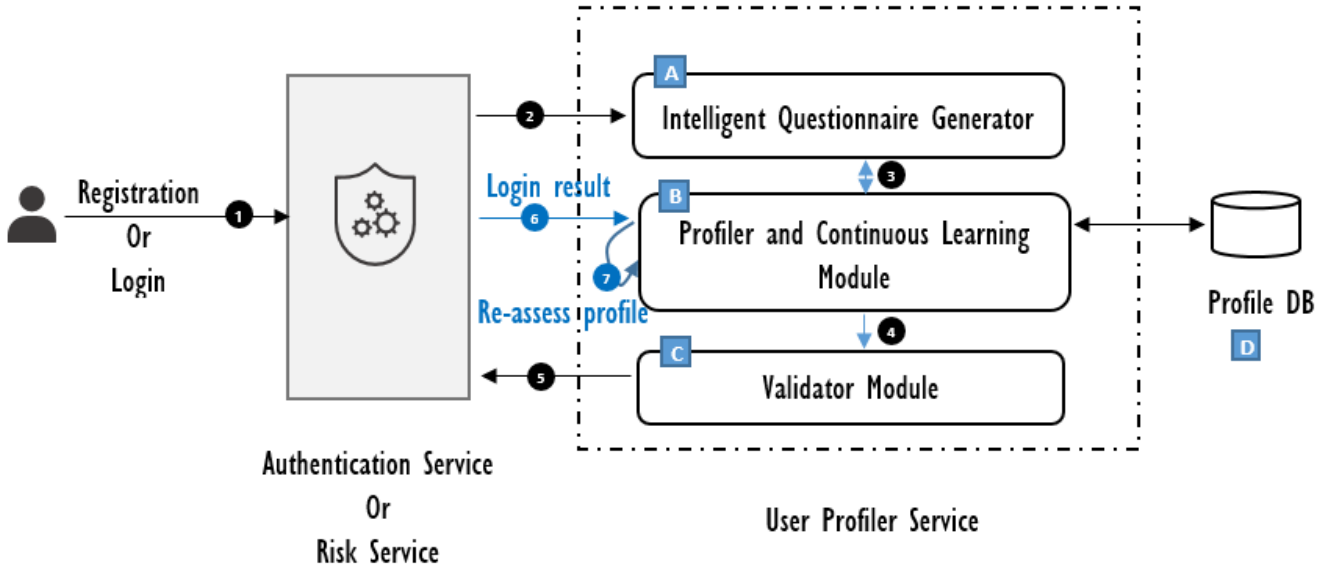


Fig 1 – Components and Interactions Design

The User Profiler Service has 4 main components:

A *Intelligent Questionnaire Generator*

This module generates the questionnaire that is used during user on-boarding and logging.

- User registration: Generates a larger set of generic questions to help build a high level profile about the user – his personality, values, interests, experiences and perceptions.
- User login: Generates a tailored set of questions based on the profile.

This module generates derived questions dynamically based on the user profile (to validate) and gaps in the profile (to strengthen). The questions are mostly pictorial to improve user experience.

B *Profiler and Continuous Learning Module*

This module interprets the user's responses to the questionnaire and creates the Uniqueness Quotient or the Personal Identity of the user. It is also continually learning and fine tuning the profile during each login request.

C *Validator Module*

This module is invoked during user login. It compares the generated profile for the user logging in with the saved profile of that user. If the profiles match within the acceptable accuracy, then returns the OK.

1) **Model Retraining** - As characteristics, perception etc of a person changes over time, this module takes care of retraining the model overtime with changing circumstances
2) **Profile Match Criteria –**
   As we are dealing with personality, perception and traits, assessment for a match can in some cases need a probabilistic approach. Instead of saying NO or YES to match for a trait. We can calculate and provide the percentage match. E.g If 90% of traits match, we can add less risk to the authentication compared to 70% match, where we will add greater risk score. Accordingly risk or adaptive authentication engine can decide whether to go for step up or allow access.

D *Database*

Stores the user profile data. It could be an extension of the User store or could simply integrate with it.

Mechanism: User On-boarding

User will fill out a questionnaire as part of the onboarding process. To limit the number of questions asked, the questionnaire will focus on assessing:

- User's personality and past experiences
- Significant other's personality and past experiences from user's perspective

These factors (personality, past experiences and perception) help in building a high level profile of the user. This profile will be fine-tuned during subsequent logins.

Note: Instead of profiling just one significant purpose, this method can be extended to profile any number of significant people in user's life. More people's profiling adds more strength to this method, however may require time to onboard user.

Variation in Onboarding:
Lower onboarding time and stronger profile overtime

In this invention we recommend to profile a person and his significant one's perception based on traits like personality, values, experiences and interests (see topic ***Uniqueness Quotient Calculation below)***. While onboarding a user we can just ask questions about personality traits. When he logs in next time, we can validate him based on the derived questions related to the traits identified during onboarding i.e. personality. If he successfully validates himself we can ask more questions related to other traits related to his experiences, values, interests in subsequent successful logins and build users profile overtime.
This will help to reduce onboarding time and strengthen user's profile overtime.

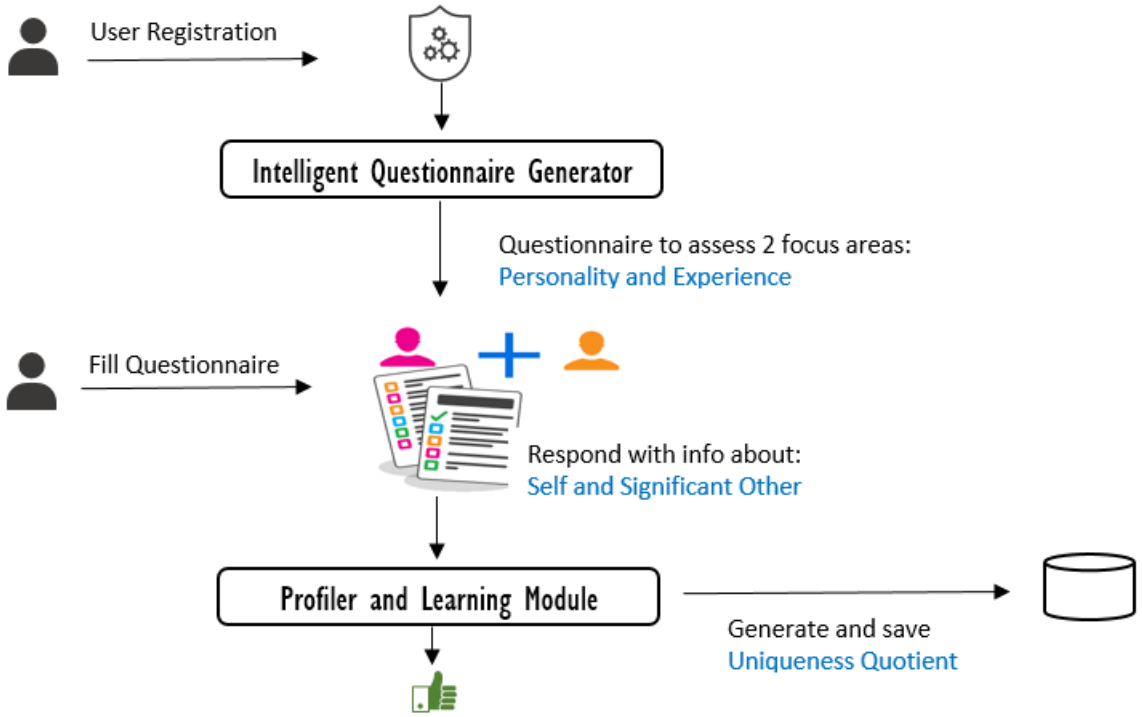


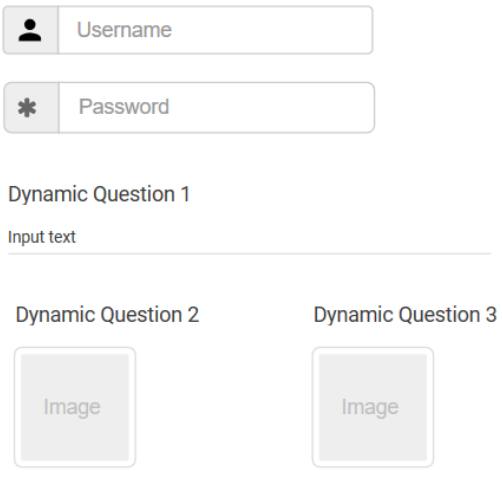
Fig 2 – User On-boarding Flow

Mechanism: User Login

This invention can be used in adaptive authentication to risk at the time of authentication. It can be clubbed with any other standard authentication mechanism. During login, user can be prompted to answer profile based questions. This is in addition to the usual authentication mechanism like username password. The Questionnaire Module presents three questions based on the user's profile:

- Question to validate the profile of the user
- Question to validate the profile of the significant other
- Extra Question to learn more about the user, to fill in the gaps in the profile.

These questions are derived based various aspects of the user's profile. They can be represented in words or as images like captcha that user needs to click on the appropriate squares.



The assessment of these questions help find the risk associated with the current login:

1) Ask username password and few dynamic questions related to few user's traits. If username password are incorrect deny him Access.
2) If username password is correct and answers to dynamic questions are correct, allow him access.
3) If username password are correct but answers to dynamic questions are incorrect, ask him more rounds of detailed dynamic questions related to his other personality traits. If those too incorrect, deny him access. Otherwise if the answers are correct, learn from the wrong assessment, update user's profile and allow him access. This method takes care of changes that happen overtime in user's personality, characteristics and perceptions and will retrain our model with time.
4) As we asked some extra dynamic questions at the time of login along with the questions required for validation, if the user logins in successfully, we can learn more details and traits about the user and his significant one and enrich our recorded profile of the user.

User Login Flow

Dynamic questions during login helps in two ways:

1. **Adaptive Authentication**: Adds to user risk and leads to appropriate action if user profile does not match.
2. **Continuous learning** and adjustment of user's profile.

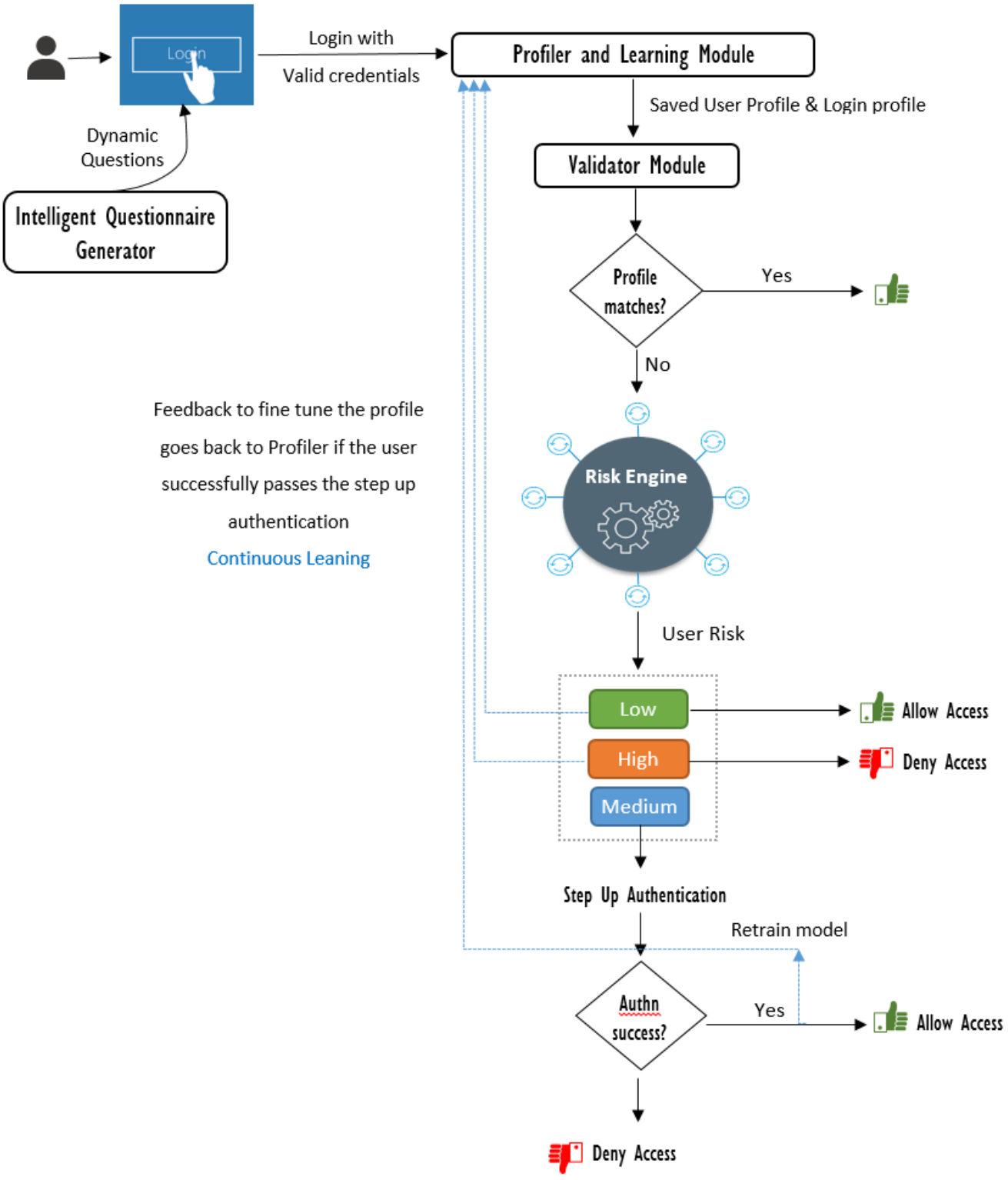


Fig 4 – User Login and Continuous Learning Flow

Variation Use case: Dynamic Security Questions

This invention can be used to add dynamic questions in current security questions authentication mechanism to make it more robust as following:

Method:

1) Ask few static security questions and few dynamic security questions based on few personality traits of user and user's significant one's profile as shown below.
2) If the answers of static questions are wrong – deny access.
3) If the answers of static questions are correct but that of dynamic questions are incorrect, ask him one or two round of more detailed dynamic questions related to his and his significant one's profile other traits. If answers to them are also wrong deny access. Otherwise, allow him access and retrain the model as we made wrong assessment on previous dynamic questions.
   This is will take care of changes a person may have in his personality, characteristics, perception etc. and will retrain our model with time.
   As we asked some extra dynamic questions at the time of login along with the questions required for validation, if the user logins in successfully, we can learn more details and traits about the user and his significant one and enrich our recorded profile of the user.

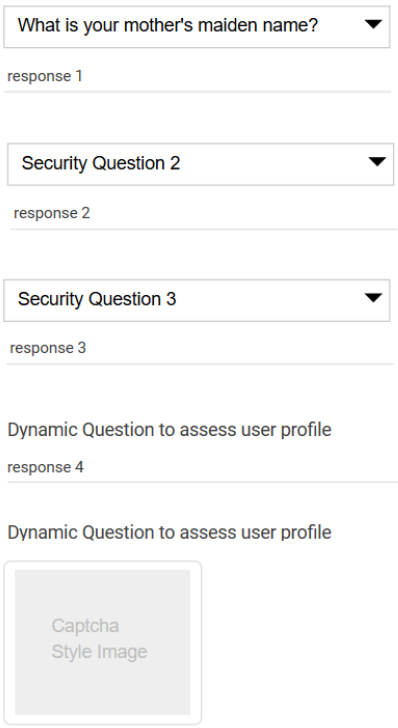


Fig 5 – Dynamic Security Questions UI Validation Flow

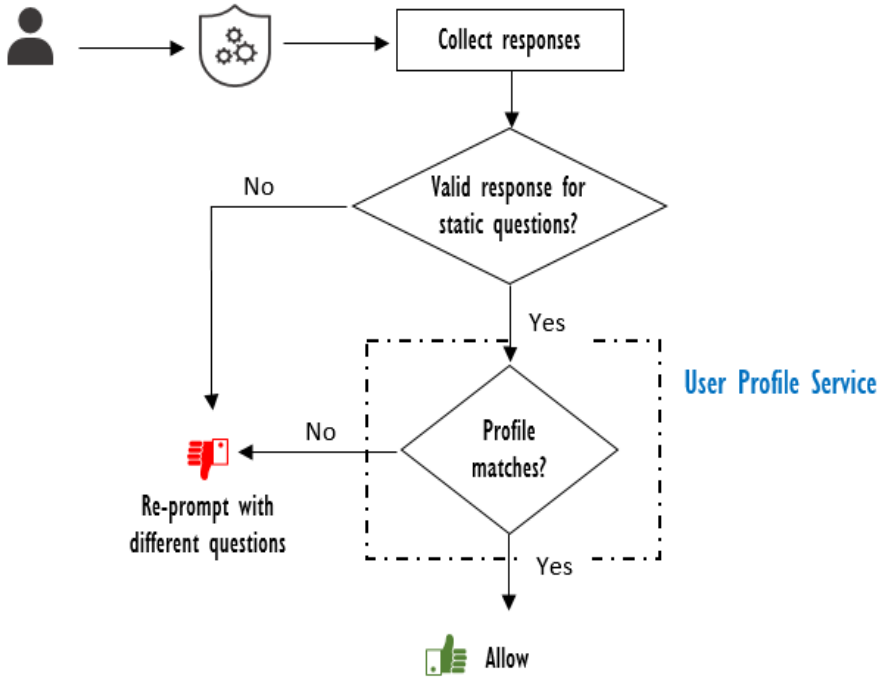


Fig 6 - Dynamic Security Questions

Uniqueness Quotient Calculation

In philosophy, 'personal identity' is the unique numerical identity of a person that remains constant over a period of time. This is also known as the Uniqueness Quotient (UQ).

Typically IAM solutions consider only the external traits like name, gender, designation to identify user. There are various other aspects that make a person unique. These are internal to the user. This information is not readily available and consequently not easy to hack or impersonate the user.

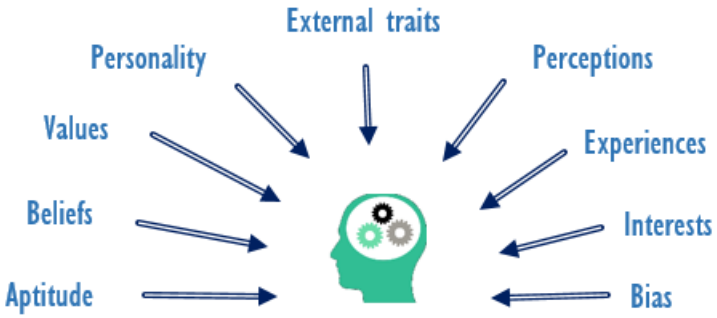


Fig 1: **Personal Identity Aspects**

We can calculate the Personal Identity / Uniqueness Quotient (UQ) by considering the following aspects:

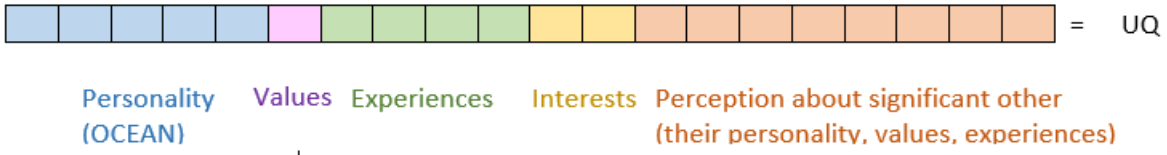


Fig 7 - Data structure to store the Personal Identity

The five areas considered are:

i. *Personality*

Today, many researchers believe that there are five core personality traits. Evidence of this theory has been growing for many years, beginning with the research of D. W. Fiske (1949) and later expanded upon by other researchers including Norman (1967), Smith (1967), Goldberg (1981), and McCrae & Costa (1987). According to these researchers, the Five-Factor Model of personality is denoted by the acronym OCEAN - Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism.

Every person has varying levels of each personality, some more dominant than the others. Users are tested for all 5 personality traits and are rated on a scale of 1 to 10 for each trait. Hence someone could score O=4, C=7, E=4, A=5, N=1. This combination is unique for each individual.

ii. *Values*

The Values Scale (Super & Nevill, 1985) was developed as part of the multinational Work Importance Study (WIS), a project supported by researchers in countries world-wide. The original values scale measured 21 values including altruism, authority, autonomy, creativity, cultural identity, economic security, life style, personal development, physical activity, physical prowess, prestige, risk, social interaction, social relations, variety, etc. Several scientists have supplemented the original study by creating their own scale or by deriving and improving the original format.

Users can be evaluated for a selected set of values and rated on a scale of 1 – 10 for each value. A combined value score will be derived for the user after assessment.

iii. *Experiences*

Users can be queried about the various experiences they have had:

- Places lived or travelled
- Activities – trekking, camping, skiing, scuba diving, etc.
- Enjoyable moments – movies, concerts, backpacking, organized travel, clubbing, playing games, etc.

- Other significant experiences – public speaking, loss of someone, moment of courage, etc.

Users will be presented with multiple options for each of the 4 experience groups listed above. They can select any number of options that apply to them.

iv. Interests

Users will be presented with various options to gather information about their interests. The data is collected in two levels of granularity – generic interests (some interest is there, but not fully pursued) and specific interest (high level of interest that is pursued).

v. Perceptions

The perceptions of a user are the hardest to guess, even by those very close to that user. Adding this to the considered qualities really strengthens the personal identity we are capturing. To keep it manageable, user will be asked about his perception about a significant person in their life – spouse, parent, sibling, friend, etc. User will be asked about this person's personality, values and experiences.

In essence, we are profiling two people – the user and the significant other. As the identity of the other person is created from the user's perspective, it may not be the same as the original identity of the other person. This difference from reality makes it more unique.

Prior Solutions

1) Security Questions - **Robust than static security questions** – (https://en.wikipedia.org/wiki/Security_question) Static security questions like "What is your mother's maiden name" are asked as part of Authentication using Security Questions and more commonly for the Forgot Password scenario. These static questions are typically easy to crack. This mechanism can be strengthened by adding dynamic profile based questions to the mix

2. Stronger Authentication Method or Risk based Authentication Mechanism – As it deals with 360 degree view of a person and takes into account his traits, personality, perception etc. It's extremely hard to crack.

Please refer point Advantages section above