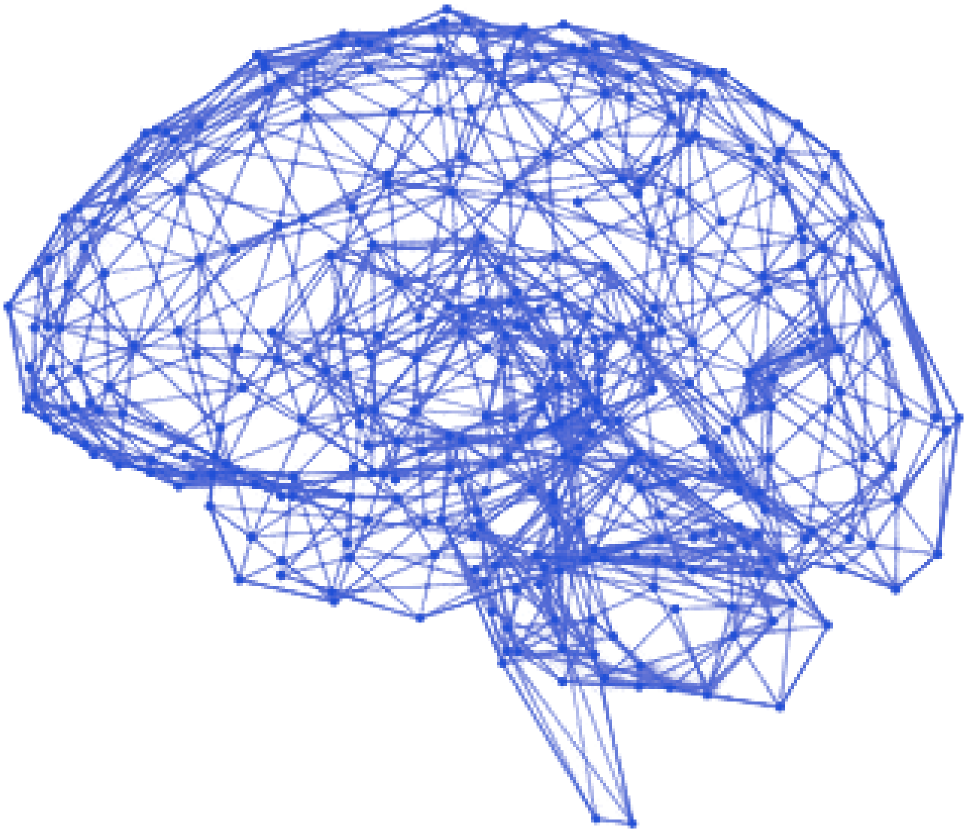
ISSM

iVerify - WhitePaper

A guide to digital identity verification



June 2022

→ issm.ai

ISSM

iVerify - Digital Verification

WhitePaper 2022

Executive Summary

I-Verify

User Authentication tool that offers fraud detection on behavioural patterns

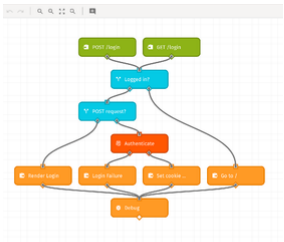
User authentication platforms include contactless biometric, facial authentication, document verification, and voice biometrics. All of these platforms although available in the marketplace but fail to provide a suite that connects these individual components together and provides usage statistics for fraud prevention. I-Verify enables organizations to build their own custom-built authentication pipelines with behavioral anomalies detection to ensure a secure user authentication system.

How Does I-Verify Work?

I-Verify enables organisations to deploy different user authentication tools across their applications. I-verify provides users simple to use workflows to manage security and tracks user behaviour to find anomalies and alert any suspicious activities.

User Authentication Tools

1. Contactless Biometric
2. Facial Authentication
3. Document Verification
4. Voice Biometric



Workflows for Authentication plug-in

Ability to deploy verification tools across channels with a simple plug-in

Behvaviourial Anlaysis

Fraud techniques in each organisation is different and hence behaviour analysis with anomaly detection enables an additional layer of security.

Executive Summary

With Pakistan's traditional businesses readily digitizing and digital businesses proliferating themselves, there is a significant need for identity risk management. Both these businesses need to assess their risks for onboarding users accordingly, especially as most operations are done remotely.

The digital world poses the same threats that the classical one does; service misuse, misinformation, identity fraud, and money laundering are common malpractices. Businesses want to provide quick services but also identify misuse of their services. Unfortunately, no one in Pakistan can manage this trade-off.

Local users, becoming more digitally literate, have similar concerns about the security of their information due to the ease of duplication or forging data. Data breaches have become the norm rather than an exception. Only recently, some of the largest financial institutes in Pakistan came under large orchestrated scammer attacks.

Verifying a person's true identity persistently is the only solution.

We must let companies authenticate users by collecting and combining their legal identities with biometric analysis. Doing this nationally can be difficult and a human-only approach can never give perfectly accurate results at that scale. This is why all previous attempts at authentication have failed. However, the advancement of artificial intelligence (AI) and machine learning (ML) techniques can solve all relevant problems. Any business can onboard any user with an identity document and an internet connection.

Consequently, this white paper will explain the ML techniques behind ISSM’s market-leading technology.

AT A GLANCE

→ Increasing need to monitor risks in a digital world

→ A robust identity verification system is required

→ ISSM's Advanced AI and ML will drive us toward that direction

Background

Smartphone penetration has crossed a staggering 100 million mark in Pakistan. Users are slowly, but in large numbers, gravitating towards a seamless digital experience. Pakistan is following the global trend of replacing shopping and banking with e-commerce and digital banking. The need for in-person interaction is deteriorating.

International transfers, P2P payments, cheque cashing services, and loan origination—all these transactions can swiftly be conducted on a smartphone. Consequently, large financial institutions in Pakistan are slowly embracing the smartphone and its never-ending convenience. The potential for the phone as a document scanner alone is bizarre. Most users will flock to their phones when they realize that they can deposit a cheque through them.

Aside from financial services, the growing start-up culture in Pakistan has opened avenues in cloud storage, web development, payment processing, payroll services, and much more.

Naturally, more online services mean more consumer data. Companies having an unprecedented amount of data are inept at managing it. This leads to breaches and reduced consumer trust. If anyone can easily mimic anyone else, stolen credit cards and fraudulent payments become impossible to stop.

Businesses seek to ascertain user-provided information in an effort to overcome this obstacle. The user may register accounts and conduct transactions online if the company establishes the user information as legitimate. This process identifies the user and confirms that the company is managed in accordance. But it's challenging to implement without delay the registration process. There is a trade-off between security and speed.

There are two fundamental ways to implement these protections:

- A very heavy initial vetting to provide assurance that users are known identities, and that they don't have a previous history or potential of conducting a financial or service crime. This initial vetting is called identity verification and is the core focus of this white paper.
- A lighter-weight vetting that can yield a lower level of service access, but that's coupled with a higher monitoring of the user's behavior once they're in the system. Assuming over time that they don't trigger additional risk thresholds, they can be granted higher levels of service access.

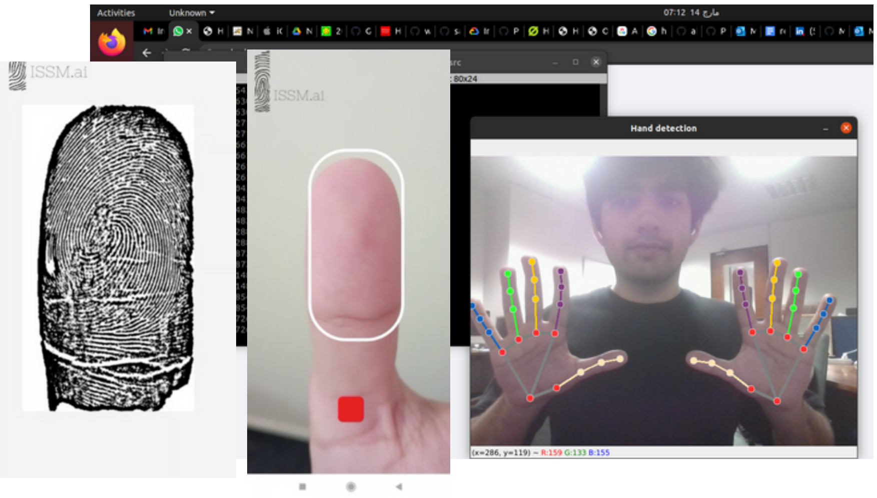
The next sections will analyze various methods businesses use to verify identity information online.

Methods of Identity Verification

So what are some common methods of verification and what is their reliability?

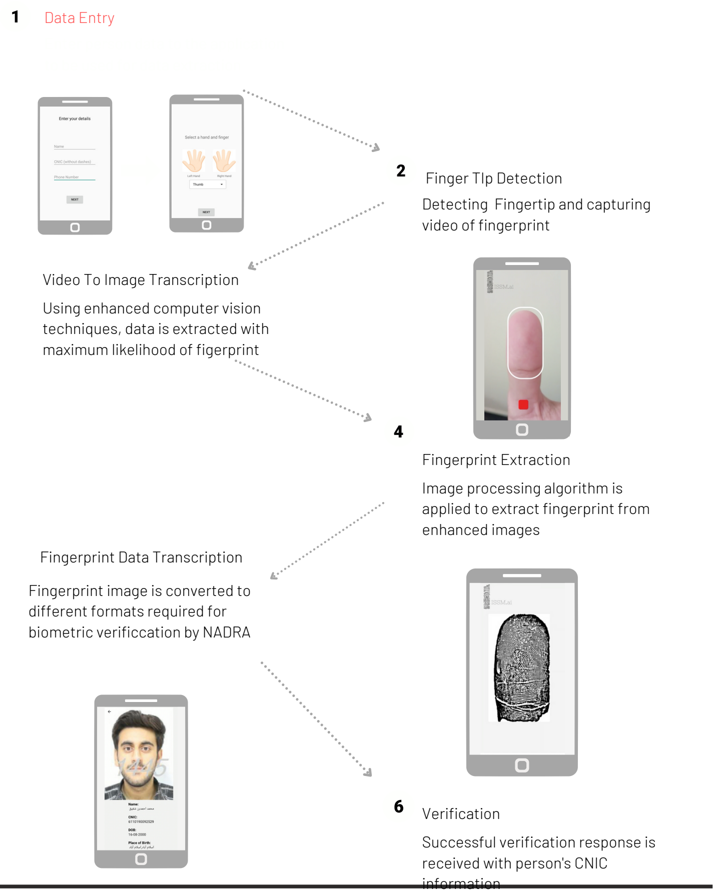
Contactless biometric

- Video Frame Detection
- Liveness Detection
- Fraud Detection
- Fingerprint Extraction
- Multiple Finger Extraction
- NADRA Approval
- SDK Built
- Android/ IOS



Cutting-edge machine learning algorithms are deployed for the detection of hand key points. This makes the fingerprint solution adaptable to changes in the verification process required by the customer.

This enables our customers to create their own respective cases for fingerprint extraction.



1 Data Entry

2 Finger TIp Detection

Detecting Fingertip and capturing video of fingerprint

Video To Image Transcription

Using enhanced computer vision techniques, data is extracted with maximum likelihood of figerprint

4 Fingerprint Extraction

Image processing algorithm is applied to extract fingerprint from enhanced images

Fingerprint Data Transcription

Fingerprint image is converted to different formats required for biometric verificcation by NADRA

Name:

CNIC: 6110190092529

DOB: 16-08-2000

Place of Birth:

6 Verification

Successful verification response is received with person's CNIC information

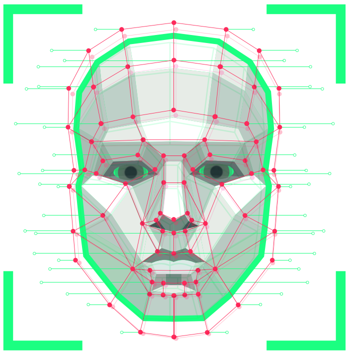
So what are some common methods of verification and what is their reliability?

Facial Biometric

Elements of User Authentication:

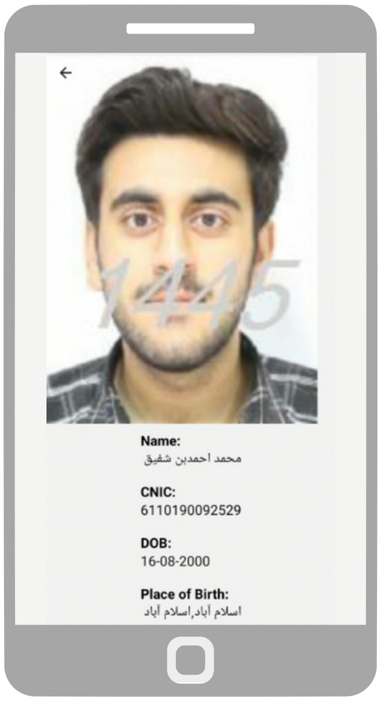
Video Calling solution uses these major elements for the identification:

1. Liveness Detection
2. Facial Recognition
3. Data extraction from CNIC



Liveness Detection

Video information captures facial data with unique markers which are used by machine learning models for liveness detection

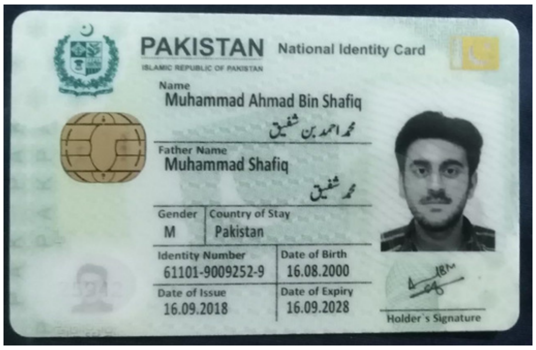


Name:
محمد احمدبن شفیق

CNIC:
6110190092529

DOB:
16-08-2000

Place of Birth:
اسلام آباد,اسلام آباد



PAKISTAN National Identity Card
ISLAMIC REPUBLIC OF PAKISTAN

Name
Muhammad Ahmad Bin Shafiq
محمد احمد بن شفیق

Father Name
Muhammad Shafiq
محمد شفیق

Gender	Country of Stay
M	Pakistan

Identity Number	Date of Birth
61101-9009252-9	16.08.2000

Date of Issue	Date of Expiry
16.09.2018	16.09.2028

Holder`s Signature

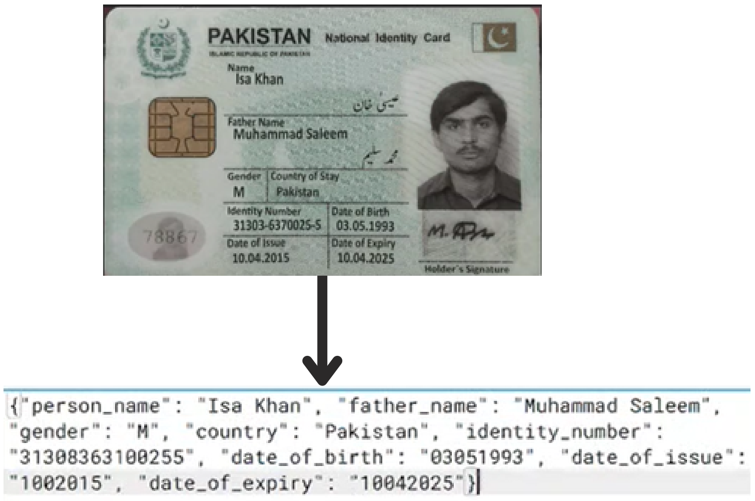
Facial Recognition

CNIC image or live authentication used to verify facial features from NADRA database. This adds an additional layer of security in case a fraud is detected.

So what are some common methods of verification and what is their reliability?

Document Verification

Document verification involves automatic data extraction and context generation from documents which can be used for document verification and relevant information extraction. It uses computer vision algorithms that intelligently identify which part of the document contains the text for data extraction. NLP and NLU algorithms are further used for text summarization and data retrieval.



PAKISTAN National Identity Card
ISLAMIC REPUBLIC OF PAKISTAN
Name
Isa Khan
عیسیٰ خان
Father Name
Muhammad Saleem
محمد سلیم
Gender M
Country of Stay Pakistan
Identity Number 31303-6370025-5
Date of Birth 03.05.1993
Date of Issue 10.04.2015
Date of Expiry 10.04.2025
78867
M. Ain
Holder's Signature

```
{"person_name": "Isa Khan", "father_name": "Muhammad Saleem",
"gender": "M", "country": "Pakistan", "identity_number":
"31308363100255", "date_of_birth": "03051993", "date_of_issue":
"1002015", "date_of_expiry": "10042025"}
```

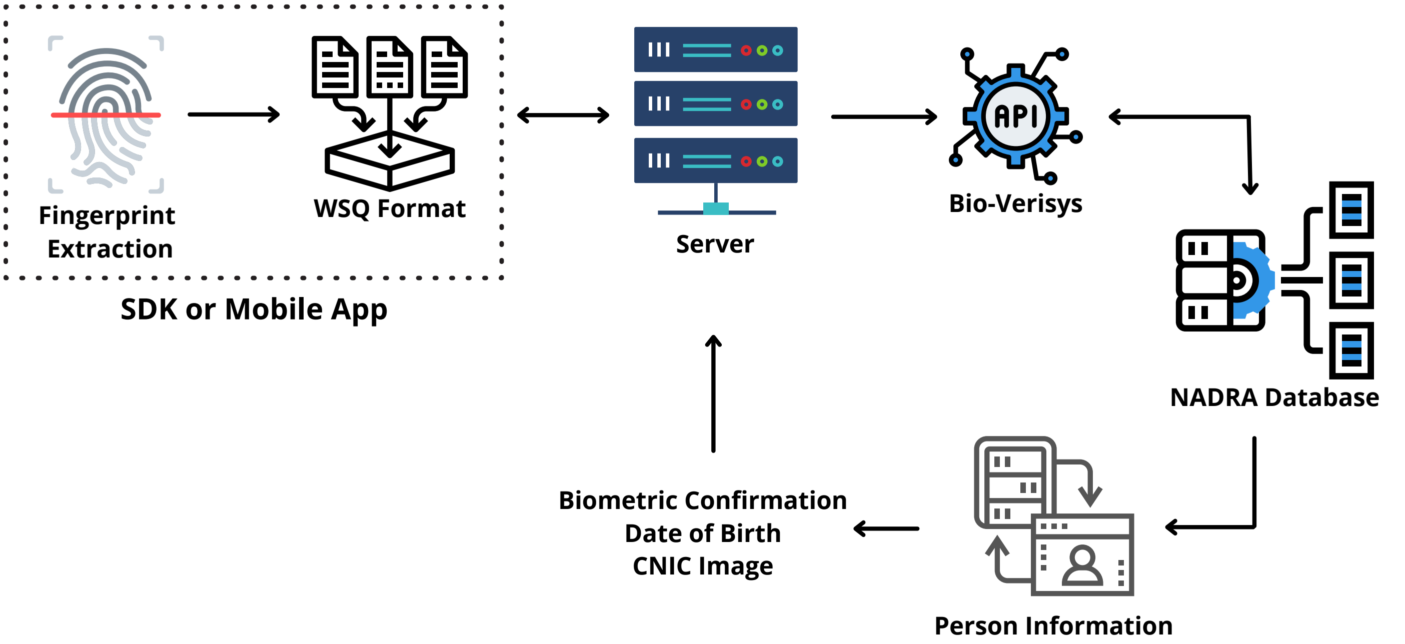
Voice Biometric

I-verify provides a REST API-based voice verification solution designed specifically for contact centers and banking or fintech apps to enhance them with an intuitive security layer. Based on voice biometrics, rather than additional security questions, customers can be verified over the phone or app conveniently.

Aside from natural, voice biometric authentication, the solution helps businesses meet various international security regulations, such as PSD2, as well as SBP regulations for KYC for larger transactions while shortening the authentication phase of an average call by 30+ seconds, significantly reducing contact center costs.

I-verify platform is a risk engine that combines various signals to assess whether a user is in fact the person they claim to be. The platform uses global identity documents as a primary source of identity and compares them to digital capture of the user in either a photo or a video. Supplementary databases can provide additional verification or augmentation of identity attributes.

While we carry user authentication, we look also for any behavioural anomalies such as IP address, MAC address, GPS location and other data points to create statistical models for any fraud.



SYSTEM ARCHITECTURE

ISSM Labelling Solutions
Csquare Pvt Ltd
Wahab@issm.ai
hammad@issm.ai

Document made by :
Abu Abdullah Ashar – Chief Product Officer

The End