July 2016

Identity Matters

International
Biometrics+Identity
Association

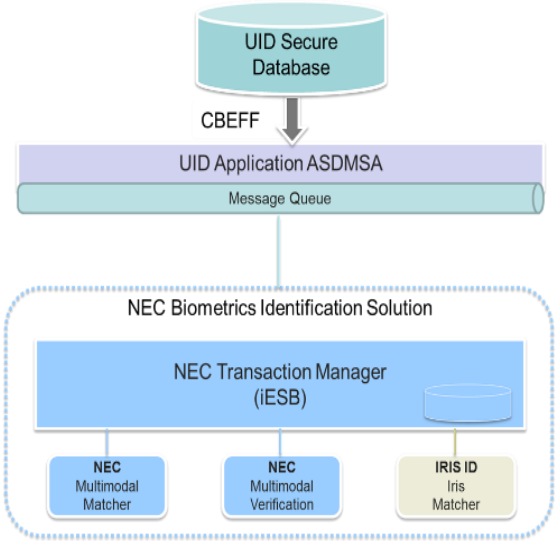
Presented by
Benji Hutchinson
Senior Director, NEC
Washington DC Operations

IBIA • Biometrics + Identity

Implementing a Large Scale Biometrics System

Example: India National Identification Program (India IUD)

- Large-Scale Multimodal Biometric System
- Multipurpose social services identification number
- Finger, Face and Iris
- Goal: Enroll 1.2 billion people in India
  - 1/6th World Population
- Workload: 1 million enrollments/day



Large Scale Implementation Issues

Accuracy

- Collecting face, iris, and fingerprints with the highest quality
- All quality degradation factors must be considered when developing matching algorithms

Optimization

- Optimizing multiple modalities requires knowledge of each biometric technology
- Fusion matching increases accuracy, but decreases search time

Large Scale Implementation Issues

Scalability

- Refers to number of enrollments and searches
- Intensity of the searches is difficult to predict

Building a High-Availability Environment

- The implemented system must mitigate all fault occurrence risk

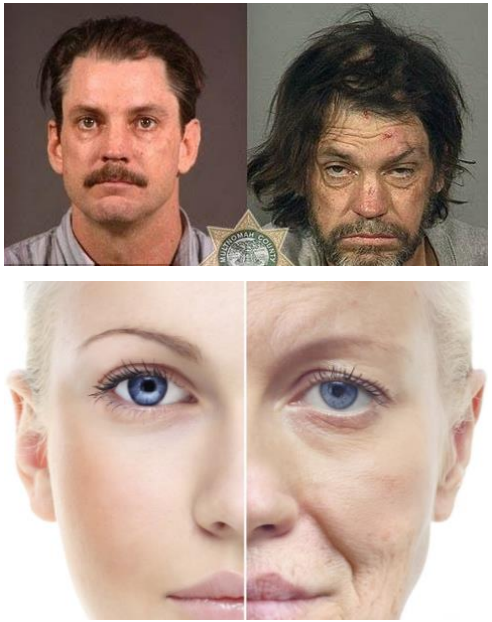
Multimodal Authentication Accuracy

- **Large data collection team is deployed to reduce launch time**
  - Quality of data depends on team members
- **Biometric information varies on occupations**
  - Blue collar workers have damaged fingerprints
- **Facial hair decreases accuracy**
- **Accuracy Calculations**
  - False Acceptance Rate (FAR) – security index
  - False Rejection Rate (FRR) – usability index

All conceivable quality degradation factors must be considered to develop a cohesive matching algorithm

Authentication Processing Optimization

- **Aging and prevailing conditions lead to imprecise matches**
- **Duplication checking**
  - Information taken at different times may not match
  - To confirm there is no duplication, the entire database must be searched
  - E.g. India UID: Checking duplication in 1.2B database requires $7.2*10^{17}$ operations
- **Optimize by only using minimum required number of parallel match combinations**



Scalability

Scale Related Factors:

- Number of people enrolled
- Number of applications used in one system
- Limitation on people to be able to be enrolled
  - Due to religion, race, disabilities, diseases, etc.
- Number of Access Points
- Degree of control

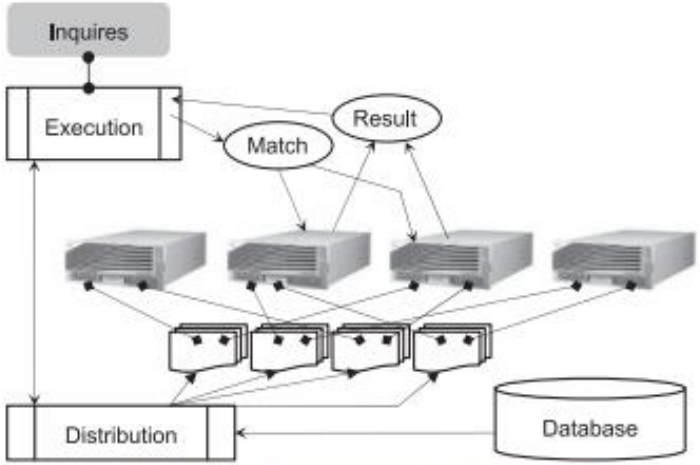


Fig. 1 Image of distributed processing configuration.

Scalability

To ensure scalability, control logic of the matching servers needs to be provided:

- With scale-out capability and scale transparency

Utility of increasing servers decreases per additional server

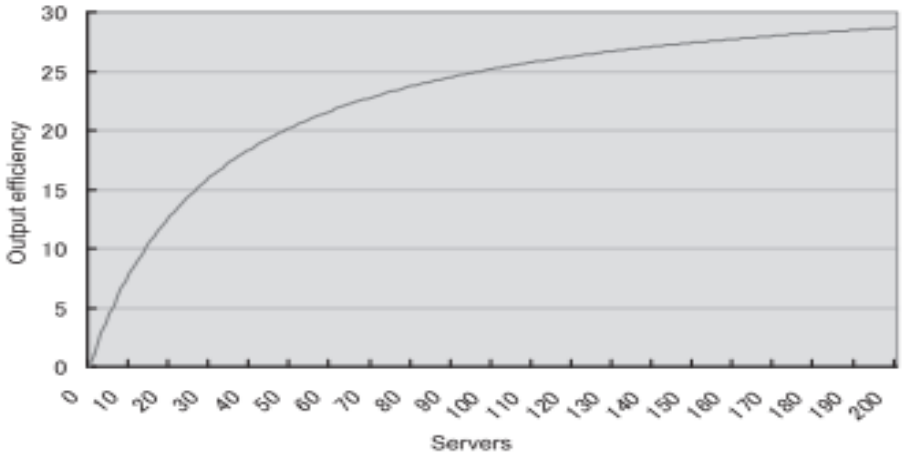


Fig. 2 Limit of scalability (when F = 97%).

Build a High-Availability Environment

Fault occurrence rate of this system is high in general

- Large number of servers
- Matching servers are over used
- CPU utilization rates are nearly 100%

Fault tolerant performance requirements:

- No biometric information should be lost in case of fault
- All operations should continue in case of single component fault
- Multiple data centers should be used as counter-measure/ load distribution

Other Factors

Number of purposes for biometrics is growing

- E.g. Automated identification, linking documents to biometric data
- Need to examine the use of biometric data

Increased quality of biometric reference data

- Quality of video surveillance images leads to identification without consent

Other Factors

Database ownership and interconnectivity with other databases

- Linking databases with different owners has intrinsic privacy and security issues
- Current legislation and enforcement must be sufficient to regulate data exchange

Level of organization in control of the application and data

International Data Exchange

International
Biometrics+Identity
Association

For more information please visit
our website: **ibia.org**