

Biometrics and Ethics - EU Project RISE

DSCI a participating institution in the RISE Consortium

1. Biometrics technology and applications

Biometric techniques provide a highly-secured and robust identification and personal verification solutions to many challenging problems in security. Biometrics is becoming increasingly common in establishments that require high security such as state security and financial sectors. The increased threat to national security by terrorists has led to the increased usage of biometrics in many countries. Unlike traditional authentication techniques, such as PIN code or password, biometrics provides an alternative way for personal identity authentication. Biometrics handles authentication of individuals on the basis of biological and/or behavioural characteristics. The major biometric features include voice, face, fingerprint, irises, retinas, palm-print, vein pattern, signature, and so on. In general, there are two types of biometric authentication processes: identification for identifying an unknown biometric token as belonging to one of people (registered in the system) and verification for accepting or rejecting the identity claim of a person based on an input biometric token. These systems make use of a number of biometric devices that capture biometric measurements such as fingerprints, palm veins, retinal scans, keystroke, voice recognition and facial scanning.

Its dominant use is in security and access control applications to mean measurable physical characteristics of a person that can be checked on an automated basis.

Biometric devices offer improved convenience and security. The devices on the front line in biometric identification setups do not get tired, unlike humans, and they are not prone to mistakes. The result is a reliable, speedy, highly accurate identification process. The field of biometric security is moving beyond mere fingerprint readers and producing more sophisticated devices that are more difficult to dupe. For example, providers are moving with hardware that senses blood flow beneath a handprint and software tools that analyze not only the password a user types in, but also how he or she typed it.

Applications include the national identity cards; tokens for authentication at the workplace and for authorization to access areas, use devices; money transfers in banks, Vein patterns are included in ATM Smart cards for extra layer of security to every transaction; hand-geometry scanners to allow access to restricted areas such as at airports; "trusted traveler" programs that allow enrolled members to use their eyes as biometrics at border crossings and customs checkpoints; e-passports with biometric identifiers; identity verification in retail stores and so on. The leading edge applications are as follows:

- Fingerprint scanners have already been installed in laptop computers and PDAs
- Sensors installed in automobiles can identify the driver, and adjust mirrors, seat positions and climate controls
- Special readers can measure various elements of hand geometry, comparing the result with data on file for each person
- Surveillance cameras can search crowds for missing persons or criminal suspects
- Face recognition software can be modified to recognize gestures, leading to improved assistive technologies for quadriplegic patients
- Vein patterns scanning being contactless, can be used where even fingerprint fails and also offer liveness test which requires active blood flow, thus making the technology spoof-proof.

2. Biometrics and privacy concerns

While biometric applications are increasing by the day, the use of this technology is raising a variety of ethical concerns with biometric identification methods, and on how this data will be stored and used. Some of these are as follows:

- Some biometric identification methods are relatively intrusive (like retina scans)
- People associate the gathering of biometric information like fingerprints with criminal behavior
- People tend to feel a loss of privacy or personal dignity, since detailed biometric information has been traditionally gathered by institutions like the military or police
- People feel embarrassed when rejected by a public sensor
- People have psychological resistance for contact based sensors like fingerprint, hand geometry, etc., in public places especially during widespread disease like swine flu.
- Automated face recognition in public places could be used to track everyone's movements without their knowledge or consent.
- Privacy concerns if the data is not protected properly and falls in wrong hands
- How will masses of biometric data be stored? Since such data can be easily moved and duplicated, how will this information be safeguarded?
- Who will have access to this information? Will companies be allowed access to face biometrics, letting them use security cameras to positively identify customers on a routine basis?

As countries are seeing increased use of biometrics technology and applications, privacy concerns and ethical issues are gaining prominence. Some of the applications, and collection and storage of data are seen to be in violation of privacy principles enshrined in privacy laws such as the EU Data Protection Directive.

3. Project RISE

It is these issues on Biometric and Ethics that led to the launching of **Rising Pan-European and International Awareness of Biometrics and Security Ethics (RISE)** – a 36 month coordinating project by the European Union with the aim of promoting Pan-European International Awareness on ethical aspects of Biometric and Technologies. The Project is picking up on the

international dialogue that was started by the international conferences on ethics and biometrics organized by the EC DG Research in Brussels in 2005; and by the US DHS Privacy Office in Washington DC in 2006. RISE aims to deepen, enlarge and ensure continuity to transnational and international dialogue on these issues.

RISE addresses several intersecting areas, security policy-making and responses to the security threats, data protection, ethics, the principle of proportionality, biometrics and security technology. These areas are expected to directly benefit by the coordination as proposed by the RISE project in the following ways:

1. Coordination will create synergies and will avoid the duplication of efforts.
2. Through the exchange of information, coordination will raise the knowledgebase of policy-makers and security researchers.
3. Coordination will help to create opportunity for new research in the field.
4. Involvement of the media and their interaction of EU Policy makers will help take the message to larger audiences.
5. Coordination with, and implementation of dialogue between the policy-makers at the international and European level, security agencies and industry will help to build a consensus.

Project RISE is in the nature of a Consortium comprising 10 partners that include 6 from the EU and 3 non-EU countries (USA, India and China). European Biometric Form (EBF) and Data Security Council of India (DSCI) are the 2 multi stakeholders that are part of the Consortium. All the inter-disciplinary competencies needed to fulfill the project objectives that include ethics, technology, politics, social sciences and international affairs, economics are represented through these 10 partners. As part of this project, an international conference in China will be hosted in early 2010. This will be the third conference - the first 2, as noted above, were held in Brussels and Washington DC.

As part of the work plan of RISE project, DSCI will do the preparatory work through a conference that is proposed to be held towards the end of September, 2009 in Delhi. There will be participants from each of these 10 Partners institutions. The preparatory meeting will provide an opportunity for RISE partners, selected Asian stakeholders, EU and US agencies to contribute to the development of China conference agenda. The meeting will be around a theme of identifying and defining the differences between nations that drive assumptions upon which security and biometric policies are based. The meeting will focus on the following:

- Differences and commonalities between ASEM States and the EU and the US as per ethics and privacy of biometrics and security technologies
- Privacy and Data Protection standards for India's IT and ITeS – BPO industry according to DSCI

Participants will include RISE partners, selected experts invited by the Project up to a max of 25 people in total.

Initial inputs for the conference: Short introductory paper, to be distributed in advance, synthesizing the main outcome of the meeting in a report to be disseminated in preparation of the Chinese Conference.