Essay on biometric technology implementation

Law, Security

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Suitability of biometric technology

The 9/11 had a profound impact in the world on security and the threat terrorism posed in a modern age. Airports around the world knew that they had to overhaul their existing security measures to ensure such mishaps are averted. The infrastructure of bridges, tubes, stock exchanges, landmark sites are ever more vulnerable than before. The issue of illegal immigrants took precedence to ensure that no illegal activity took place. Security in the western world acquired a new measure of urgency. This essay looks at " biometric technology" as a verification and identification device.

Senator Charles Schumer who was working on a bill to enforce biometric cards to workers in the United States observes in a newspaper article," Our immigration system is badly broken. We have no way to track whether the millions who enter the United States on valid visas each year leave when they are supposed to. And employers are burdened by a complicated system for verifying workers' immigration status."

It is estimated that over 11 million people enter America illegally, there is just no accounting as to what these people may do including drug trafficking. Any unlawful activity by immigrants must warrant immediate deportation and a need for a reliable verification and tracking system to ensure greater efficiency.

An effective employment verification system would aid in making employers accountable when they hire workers; they must have access to a database as to the legality while recruiting. A tamper-proof ID system, like a biometric, would dramatically reduce illegal immigration or those who overstay their visas.

IS THE CURRENT TECHNOLOGY EFFECTIVE?

The password is simplest and cheapest requiring elementary software resources.

But this system is vulnerable to attack; easy to extract by hacking the software. For instance, a program that simulates the “ user name and password” window can induce the user to part with his data and that is misused as in bank accounts. This is called phishing and bank always warn their customers to be careful in their online transactions.

The Smart Cards are an effective authentication alternative and more secure than a password. The chief drawback its small size and that limits more date inclusion for want of storage space. Besides it comes with the danger of being easily lost or stolen and it can be manipulated.

The typical identification methods necessitate a person to carry something -- an ID card, a personal identification number (PIN), or password –these come with a risk of being replicated or used for a fraudulent identity. Biometrics, on the other hand, is more reliable – though not hundred percent accurate – and not easily falsified or stolen. This is due to the fact that biometric identifiers are distinctly unique to a person: a 3-D image of the individual's hand, a person’s iris scan, a fingerprint impression or voice sample is distinctly unique for each human being.

MOST COMMON BIOMETRIC TECHNOLOGIES

Technology does promise a lot; sometimes a little over too. For any verification database system to be effective, the system must undergo checks on accuracy; margins of error. The cost of setting the enrolment programme based on a chosen technology and maintenance costs, user acceptance, privacy issues, etc must be considered for these would run into billions of dollars and a long term “ locked into an technology" implications

Iris Recognition: This consists of a small camera to capture black-and-white, high-resolution image of the iris. Algorithms define the iris boundaries to create a grid of the image. This is stored as the individual's biometric template in the database.

The camera image of people who sport coloured or bifocal contact lenses may make for a skewed storage template. Then there are those with glaucoma or contracts for whom the iris imaging may not yield a definitive matching. Despite these limitations, UAE government has found this very useful.

The United Arab Emirates (UAE) adopted iris recognition as a security measure to prevent expelled foreigners from entering the country again. The deported or expelled immigrants would return to their home country, legally change their name, address particulars, and acquire a new passport. They would re-enter UAE as the immigration authorities had no biometric reference to cross-check. The physical paper system was circumvented by a new passport.

They adopted scanning the iris of individuals entering or leaving the country. It was easy to use and it was proving extremely effective. Over the years around 6, 000 foreigners were found re-entering the country despite a ban. It was found so successful that UAE is considering creating a unified Arab database. It has found the iris technology so user-friendly that it is envisaged to be included in the passports of their nationals and their identity cars.
Hand Geometry: Hand geometry uses measurements of the width, height, and length of the fingers, shape of knuckles, distances between joints, etc. It uses optical cameras to capture the image of the hand. Based on these images, 96 measurements are then calculated and a template created.

The San Francisco airport uses hand geometry for allow entry into the tarmac; Scott Air Force Base, Rotterdam port, University of Oklahoma also use this technology for authentication.

Fingerprint Recognition: Fingerprint recognition makes use of the impressions formed by distinct ridges on the fingertips. These scanned images captured by optical or ultra sound scanners are converted into templates and stores.

It finds a lot of opposition on a voluntary enrolment programme as finger print causes a revulsion with a strong mental association of a criminal. Finger prints also are not effective on people whose finger whorls and ridges are worn out from age or those working in corrosive chemicals.

If there is one area where fingerprint biometrics have found acceptance is in health care for access of patient files. Users can have access to their medical records from a finger print identification. Besides it helps these patients see the data stored as a string of numbers than the actual image.

Facial Recognition: Face recognition technology identifies people from certain facial features such as eye sockets, shape of the mouth, or the jaw line. This is the sole biometric system that can be generated covertly. It is useful for surveillance, the suspect’s face can be captured on video and the image stored algorithmically on a database.

This technology has been used in airports security and the error margins have been too significant for utility.

Voice Recognition: Voice recognition technology utilises the distinct in the voice, pitch, frequency, physiological differences and speaking habits. The pass phrase is then converted to a digital format and distinctive features like pitch, tone, cadence to create a template for the sample. However the drawback of this technology it high error margins in noisy environments like in airports.

This technology has been found to be extremely useful in the US-VISIT programme. An individual’s data would be captured in the database whey

they apply for a visa at a U. S. consulate. The person is mandated to record a voice sample and a pass phrase then. Later, in the United States, this data can be used to crosscheck by the state or federal employees for verification.

Biometric Smart Card technology: Match-on-card technology can be store any biometric in a card form. The card has a biometric template (like iris or digitized fingerprint) and this when swiped can be compared to a stored database for verification. The card is scalable too if more biometric are to be added for greater security.

CIVIL LIBERTIES ISSUES – CALL FOR SAFEGAURDS

Biometrics finds a lot of supporters on the grounds of a vastly superior verification system that cannot be easily manipulated or forged. But civil liberty opponents argue passionately that it would infringe a person’s liberties and lead to loss of privacy. So many questions and objections are raised to ensure the technology is not abused.

a) Is biometric system flexible enough to different levels of verification to suit the situation?
b) Who is to monitor and administer the programme?
c) Who are the authorities that will have access to the database?
d) Is it possible to restrict access to the database to different agencies?
e) How will data be protected especially in the days when most of them are outsourced to India and China?
f) Is the system responsive to an individual’s privacy concern? And how does one ensure that the data is not misused and given to the private sector to be misused for marketing?

g) How do we ensure citizen enrol voluntarily and are convinced that the technology affords far greater efficiency in security matters?
h) Will the date be stored locally or at a central level with access at multiple agencies?

There are lots of questions that need to be addressed by the administrators to inspire citizen’s cooperation.

There is no gainsaying that biometrics provides security with a better verification system; immigrants can be better tracked to ensure that no one overstays and it also gives employers a facility to check on the legal status of their recruits. Biometrics would be especially beneficial in areas where security risks are high – airports, malls, tubes, bridges, and very visible high risk vulnerable spot. Since the biometric is so unique it cannot be easily falsified.
Unimpeded access of biometrics has a downside too; there is a potential for abuse and a legitimate concern of social activists. This technology can be abused to violate personal privacy and civil liberties. When used without permission or for those purposes than the other initial envisaged, sold to the private sector, or even for surveillance on a personal ground, it can impinge and intrude the freedom enshrined in the constitution.

Any verification system comes with a defect of wrongful tracking and these dangers must be minimized at systemic level. Today’s global environment in which terrorism is a way of our life, citizens do not mind a level of security to meet the threat. There is fine balance between anonymity and complete identification; these devices must not overreach and stray from the intended

objective. Any data collected must only to be used for legitimate government purposes and not overburden the individual with too much checks and authentication procedures that it gets exasperating.

The biometric technology must be sensitive to as many levels of gradations of verification for each purpose. Much verification can be done without divulging detailed personal information. A certain level of anonymity can be built into the system.

The government has a right only to investigate those that threaten public safety. The citizen must trust the government that exhaustive investigations on suspects are done for a good reason. Generally, most verification falls on a spectrum of total anonymity and detailed investigations - from anonymity to pseudonymity to full identity. The challenge before biometrics supporters and administrators is to convince the public that their civil liberties are not compromised or misused.

So a viable meeting ground is essential to balance to need for security to the privacy concern of the individual. A few basis pointers must be borne in mind when assessing a particular biometric technology.
Enrollment in biometric systems should be overt rather than stealth and covert. An individual enrolled must be informed about the programme and queries answered to gain confidence in the proposed system. Nothing hurts a programme’s credibility than misinformation.

Biometric systems are best operated where data is locally stored than a centralized mechanism for they tend to raise privacy concerns. Federal

access must only on exceptional basis and on solid grounds.
It must be mandatory for immigrants and visitors to a country to have a biometric identification to aid a system that they don't overstay or work without a permit. DNA screenings are required for those with criminal backgrounds or convicted terrorists.

For privacy and security reasons, it is preferable for data to be in a template form than a digital image. Besides templates are harder to infiltrate.

Similarly, where feasible, biometric systems should consider " pseudonymity" for verification where the identity of the individual is concealed by the system at least at the early layers of checks. Ideally there must be an authorization from judiciary for a penetrative access of data; where real threats persist and the additional information is critical to nail down suspects.

There must be built-in systems to ensure a limited access of data, to prevent misuse. Federal and local agencies must collect, use, information of an individual only in the case of security and law enforcement.
The principle of layered security necessitates having secondary (parallel) identification as a support to biometric systems; especially when the system provides inconclusive match or large error margins.

CONCLUSION

Biometric technologies can be embedded with suitable protocols to ensure privacy and not intrude in a person's liberties. There must be strict operational guidelines to meet the privacy concerns. The system must

ensure that law abiding citizens are not harassed with security paranoia by long lines and unnecessary verification while the system must be efficient to apprehend the real culprits.

Advanced technology should be definitely used to combat security procedures. Perhaps if there were greater co-ordination between agencies and effective surveillance at the airports 9/11 could have been averted. Any nation would do anything to ensure there is no repeat and biometrics is a technology we can ill-afford to ignore in these days of heightened global terrorist threats.

BIBLOGRAPHY

Derail Amnesty. [online] Available at http://www. derailamnesty. com/Schumer-Graham_Proposal. html [Accessed 10 June 2011]

Talk show. [radio] Available at http://www. kuow. org/mp3high/mp3/Conversation/ConversationB20100512. mp3 [Accessed 10 June 2011]

Rosenzweig, Kochems & Schwartz, 2004. Biometric Technologies: Security, Legal, and Policy Implications. [Online] Available at http://www. heritage. org/research/reports/2004/06/biometric-technologies-security-legal-and-policy-implications [Accessed 10 June 2011]

Advantages and Disadvantages of Technologies. [Online] Available at http://biometrics. pbworks. com/w/page/14811349/Advantages-and-disadvantages-of-technologies [Accessed 10 June 2011]

Zalma, A. Biometric Identification & Homeland Security – Biometrics Pros and Cons [Online] Available at http://terrorism. about.

com/od/controversialtechnologies/i/Biometrics_2. htm [Accessed 10 June 2011]

Strohm, C, 2009. Schumer proposes biometric screening of U. S. workers. [Online] Available at http://www. nextgov. com/nextgov/ng_20090625_5400. php [Accessed 10 June 2011]