Integrating Bluetooth, Biometrics and Smartcards for Personal Identification and Verification

Vivek Jain and Ramesh C. Joshi

Recent years have shown considerable growth and usage of Personal Identification and Verification Systems starting with paper photo IDs, digital IDs, smartcards and now Biometric IDs. **Every time an effort is made to make personal identification and verification more secure and reliable. However, the bottom line is that no system can be completely foolproof; the level of difficulty involved in fooling the system is the measure of its supremacy over others.**

The authorized users can gain access to secure information systems, buildings, restricted sites, etc via multiple passwords, Identity cards, personal identification numbers, secure tokens, keys, codes, etc. But, these security methods are not sufficiently reliable to satisfy the security requirements as they can be *lost, forged or forgotten* [1]. Also, there exist no easy way to monitor and store information about individuals entering public places like airports, museums, government buildings, etc which might be useful to track a person later.

With new types of terrorist attacks happening including suicidal attacks, **the changing security scenarios not only require accurately identifying the person but also preferably from a greater distance, giving the authorities more time to take appropriate action.** To this end we propose to develop a Personal Identification and Verification System, **DistanceID** (identification from distance) that integrates three technologies viz. Bluetooth, Biometrics and Smart Cards into one. The system consists of:

- Bluetooth enabled Smart Card called **IBCard** (Identity on Bluetooth Card) carried by the person, and
- Detecting device, **IBDetector** that communicates seamlessly with IBCard via Bluetooth (or it can be a simple smart card reader).

The IBCard stores personal information like *name, address, blood group, social security number and driving license, photograph* and Biometric information preferably *fingerprint and face/iris* among nine different biometrics techniques that are widely used/under investigation.

TECHNOLOGIES INVOLVED

The DistanceID combines the following three technologies into one:

Bluetooth

Bluetooth is a low cost, low power, short-range radio technology originally developed as a cable replacement to connect devices such as mobile phone handsets, headsets and portable computers. Bluetooth has created the notion of a Personal Area Network (PAN), a kind of close range wireless network enabling ad hoc connections between various heterogeneous devices. Bluetooth is emerging as the preferred wireless technology for WPAN. The only other competing technology is IrDA, which has a number of shortcomings the main being line of sight communication that make it much more difficult to use than Bluetooth. The other being 802.11 which is well suited for WLAN.

However the proposed system is expected to work within the domains of a WPAN (max. 100 m) as there is no point in identifying a person at a distance outer this domain as more the distance the greater will be the inaccuracy and interference. As in all wireless technologies *devices are identified randomly and not depending upon the distance from the detector*. So, locating direction of a person from the IBDetector in a sphere of radius bigger than the ranges of WPAN will be very difficult until we employ highly directional antennas in IBDetector.

The Bluetooth concept offers several benefits compared with other techniques. The main advantages of Bluetooth are [3]:

- The minimal hardware dimensions,
- The low price on Bluetooth components,
- The low power consumption for Bluetooth connections.

These are the major advantages as the IBCard requires the Bluetooth hardware to be placed on a smart card hence it is expected to acquire minimum space and power.

Biometrics

Biometrics refers to identification of an individual on the basis of his/her physiological or behavioral characteristics to make a personal identification, and, therefore has the capability to differentiate between a genuine individual and a fraudulent impostor.

At present there are mainly nine different biometrics techniques that are either widely used or under investigation including [2]: *face, facial thermogram, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature and voice print*. All these biometric techniques have their own advantages and disadvantages and are admissible upon the application domain. However the fingerprint as the biometric techniques is widely used and the technology has matured with time. Biometric authentication has proven to be an effective means of deterring fraud; in conjunction with smart cards, biometrics can also allow for controlled, portable access to personal information.

Smart card

Smart card is a plastic card with an embedded integrated circuit (IC) that stores and/or transacts data. The primary distinction among smart cards is whether their IC is a processor chip (CPU) or a memory chip. Processor chips, the type most likely to be commonly used in conjunction with biometric authentication, are able to manipulate data on the card for different on-board applications

Smart cards and biometrics are linked at one specific point: the storage of the biometric template. A biometric template is an encrypted hash of the actual biometric itself. Once created, the template is digitally signed and locked onto the card by the issuing authority. Physiological aspects of the face, iris, hand, or fingerprint (most common in human services) are converted into templates for ease of use. The average image of a fingerprint may require 225Kb, far too large for usage in any smart card or identification application. The template, representing distinctive measurements or features of the body part, is much smaller, and can be stored and manipulated on the card. The following types of biometric templates can easily be stored on an 8Kb smart card [4]:

- Finger scan: 250-500 bytes,
- Facial scan: 1200 bytes.
- Iris recognition: 512 bytes

Secure ID systems that require the highest degree of security and privacy are increasingly implementing both smartcard and biometric technology. As smart cards storage grows larger, and biometric technology less expensive, storage and throughput times should be no impediment.

SYSTEM OVERVIEW

Figure 1 gives a pictorial view of how DistanceID works. It involves three main agencies:

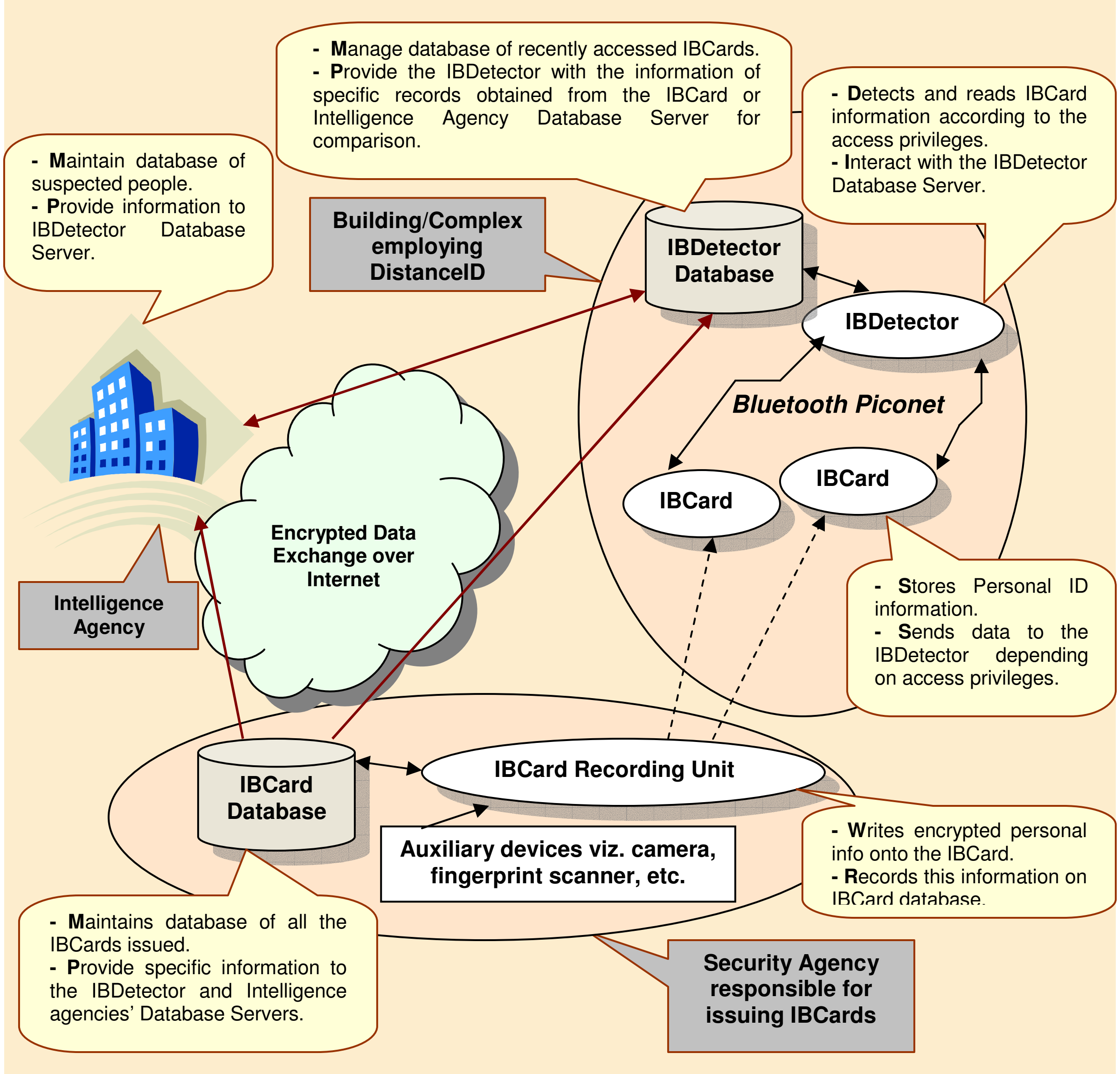

- Manage database of recently accessed IBCards.
- Provide the IBDetector with the information of specific records obtained from the IBCard or Intelligence Agency Database Server for comparison.
- Detects and reads IBCard information according to the access privileges.
- Interact with the IBDetector Database Server.
- Maintain database of suspected people.
- Provide information to IBDetector Database Server.
Building/Complex employing DistanceID
IBDetector Database
IBDetector
Bluetooth Piconet
IBCard
IBCard
Encrypted Data Exchange over Internet
Intelligence Agency
- Stores Personal ID information.
- Sends data to the IBDetector depending on access privileges.
IBCard Database
IBCard Recording Unit
Auxiliary devices viz. camera, fingerprint scanner, etc.
- Writes encrypted personal info onto the IBCard.
- Records this information on IBCard database.
- Maintains database of all the IBCards issued.
- Provide specific information to the IBDetector and Intelligence agencies' Database Servers.
Security Agency responsible for issuing IBCards

Figure 1: The System Overview

- ***IBCard and IBDetector issuing Security Agency:*** This is the main agency responsible for issuing IBCards and IBDetectors. It also maintains database of IBCards issued is expected to be employ the highest level of *information assurance* that includes the following activities [5]:
  - Creating multiple copies of database.
  - Storing these copies in different storage media and at different locations.
  - Managing consistency among these copies
  - Synchronization of records in these copies of databases.
- ***Intelligence Agency:*** This agency maintains database of suspected people. Again data integrity and security is top priority here.
- ***DistanceID employing Agency:*** As the name implies this is the agency that employs DistanceID.

The communication between the Database Servers of these three agencies is central to the effective working of the system. The data exchanged is encrypted to avoid eves dropping resulting in Identity Theft.

INFORMATION RETRIEVAL AND CIVIL RIGHTS VOILATION

As we expect IBCard to replace all other existing IDs, it is necessary to provide means for information retrieval not only through wireless means but also through existing means. The card provides information in two ways:

- **Manually:** General Information is printed on the card so that in the absence of a detector also the card supplies the necessary information.
- **Electronically:** All the required information is also stored on the smartcard memory. Memory is expected to be ROM so that in no case data on it can be tempered. The information from this smartcard can then be extracted electronically in two ways.
  - ***Contact Reading:*** Through smartcard reader information can be extracted.
  - ***Contactless Reading:*** Via Bluetooth Information is transmitted to the detecting system.

Other than hardware/software issues another big issue is that of Identity theft. The ability to detect anyone with a card without them knowing about might present opportunities for civil rights violations and criminal abuse through hacking. This problem of **identity theft** is solved in our system by using the concept of domain-based access at the IBDetector end and providing the user with Domain Protector at the IBCard end. The IBDetector is distributed under the control of Security Agency and depending on the purpose for which it is given; the domain is hard coded in the IBDetector application.

Domains and Domain Protector

We divide the information carried by the IBCard into three domains viz. ***NORMAL, SECURITY LEVEL 1*** and ***SECURITY LEVEL 2*** domains that define the access privileges of the operator (refer *figure 2*) at the IBDetector side. Depending on the domain, only the information of the allowed fields is available to the operator.

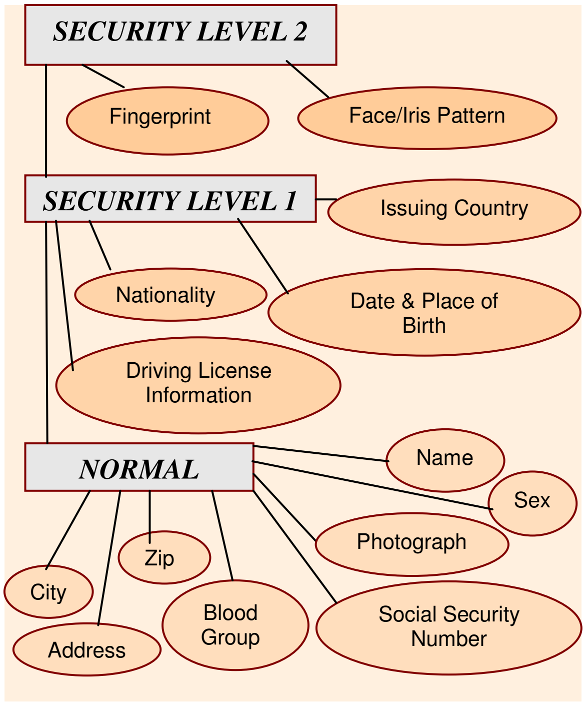
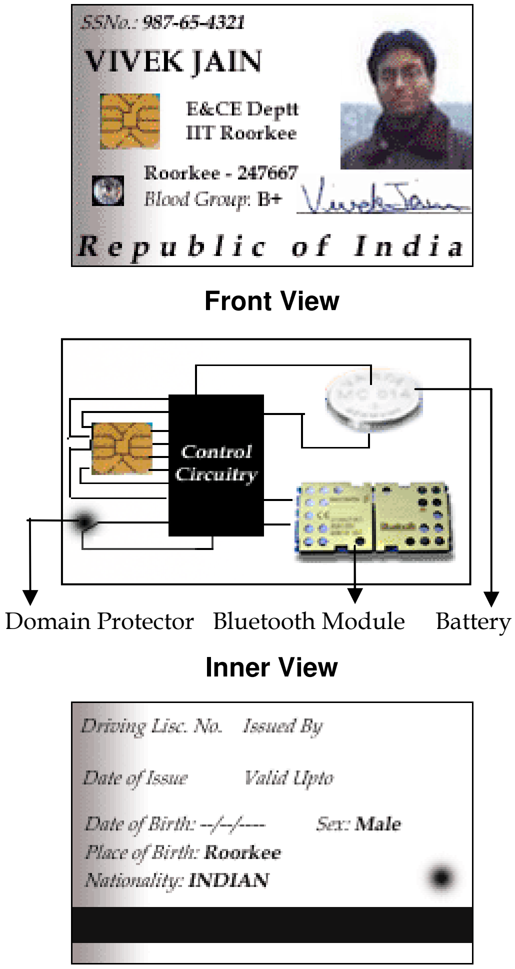


Figure 2: The Hierarchical Data Model of the Domains

The fields lying in normal domain is termed as general information that is available in all times whereas for obtaining the information of security levels user will authorize the operator for obtaining information by switching off the **"domain protector"** (refer *figure 3*). So, the user knows when his/her critical information is being accessed and by whom.

The person operating the IBDetector has to pass identity verification test before any IBCard is detected. For a detector operating in *normal mode* (used by librarians, doctors, etc) the operator can access only information under the normal domain. Whereas the ones operating in Security Level domains, the information other than in normal domain can be accessed only once the user allows after switching off the *domain protector* in their IBCards.

RSA encryption has also been provided to ensure data security so that data is available only to IBDetector and no other detectors. RSA encryption uses public and private numerical "keys" based on large prime numbers to convert text into a scrambled format. The resulting unreadable "cipher code" cannot be understood without the correct access key. When data is stored on IBCard, it is encrypted using the public key. Only the IBDetector possesses the private key capable of decrypting the information.



Front View

Inner View

Back View

Figure 3: IBCard

To authenticate the card, the physical means such as micro-printing, embedded holograms or optical laminates can also be present to avoid tampering.

OPERATING MODES AND THEIR APPLICATIONS

The system works in number of ways for various applications as desired by the organization. Here we identify the five basic modes, the system is used in:

- **Detection mode:** In this mode the individual's identity is manually verified against his/her photograph obtained from the IBCard by manual or electronic means. This mode is efficient to use at places where the security requirement is not very high.
- **Recording mode:** Under this mode the personal information obtained from the IBCard is stored on the IBDetector database. This mode provides the operator with the flexibility of selecting desired fields (allowed in the domain of working) from the available ones and storing them onto the specified database. The date and time of detection can also be recorded. In *normal domain* this mode is applicable at places like libraries, government buildings, museums, etc. where it is required to maintain an *Entry Register*. ***This mode is extremely useful in the aftermath of building collapses, train accidents, natural calamities (earthquakes, hurricanes, etc.) to detect and create database of people buried under the debris.***
- **Searching mode:** Here, a specific person in the sphere of the range is searched. In this mode user can search for person depending on all or any one of the entered fields like name, city of residence, blood group *(helpful for doctors in case of emergency)* and social security number.
- **Monitoring mode:** Monitoring mode is used in high security areas to allow or restrict a person to enter or leave the premises by verifying his/her identity information obtained from the IBCard with the stored database records in the IBDetector Database Server. This is very pertinent in restricted places like nuclear power plants, defense sites, important government buildings, etc.
- **Security mode:** This mode is a combination of Recording and Monitoring modes. This mode is applicable at places like airports where the people boarding the aircraft are constantly monitored against the stored database of criminals. Besides monitoring, this mode also maintains a database of all the people boarding the aircraft for later use if required. This also finds its application in restricted places like nuclear power plants, defense sites, important government buildings, etc.

PROTOTYPE DEVELOPMENT AND EXPERIMENTAL RESULTS

The implementation of the prototype is divided into five basic software modules: IBDetector module, IBDetector Database module, Bluetooth Communication module, IBCard Recording module and IBCard Database Server module. The prototype is implemented as:

- **IBDetector:** This component is realized by using a PC/Laptop with the Ericsson Bluetooth Module connected to it. The

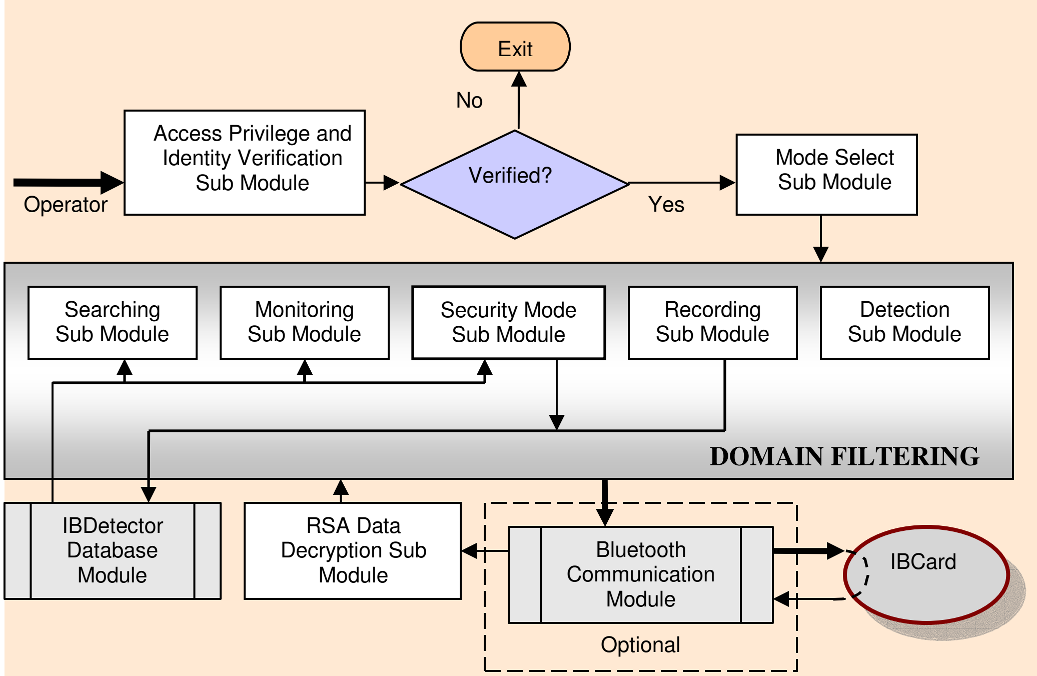


Figure 4: ***IBDetector Module Data flow Diagram***

IBDetector Database Server is also realized at this end. The IBDetector, IBDetector Database and Bluetooth Communication modules run here. *Figure 4* gives the basic data flow diagram.

- **IBCard:** With Bluetooth enabled smartcards still to come, the IBCard was simulated using a PC/Laptop with another Ericsson Bluetooth Module connected to it. Bluetooth communication module runs here.
- **IBCard Recording Unit:** The PC/Laptop used to simulate the IBCard is also used as the IBCard Recording Unit to store data in IBCard in encrypted form. The ***IBCard Database Server*** is also realized at this end. IBCard Recording and IBCard Database Server modules run here. *Figure 5* shows the basic data flow diagram.

The code for the above software modules were developed in Visual C++ and the White Box and Black Box testing was carried out and it was found the system worked well.

- It took about 6-8 sec to transfer information from IBCard to IBDetector at a distance 9m. The larger distance resulted in intermediate disconnection.
- The total information took about 3-5 KB space. Text information (200-500 Bytes), Photograph (1-2 KB depending upon the compression.), fingerprint impression (1-2 KB depending upon the compression.) enough to be placed onto a smartcard.
- During monitoring and security modes the fingerprints and photographs obtained from IBCard are compared with that stored in IBDetector database server. It has been found that there has been no bit errors while transmission over Bluetooth.

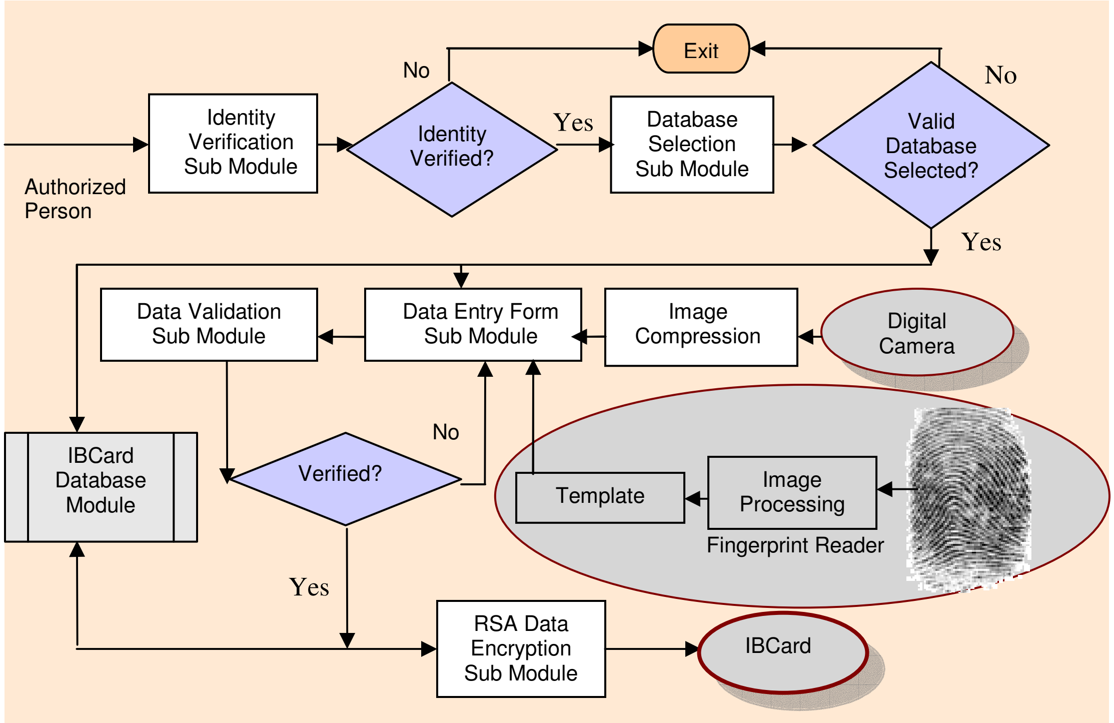


Figure 5: ***IBCard Recording Module Data Flow Diagram***

Table 1 gives provides the details for the time taken at various levels during the transmission of data in the system prototype.

Table 1: Data Transmission Time

Connection Speed (Ericsson Bluetooth Module)		**Smart card (Schlumberger 8K Cryptoflex Cards)**	
Detection (max.)	10.5s	Reading card 5KB (9600 bps)	4.2s
Selection and Connection (max.)	0.9s	**Bluetooth Connection Range**	
Transmission Time 5KB (400 kbps Av.)	0.1s	Obstructed / Unobstructed	10m/45m
Approximate Total time (max.)			**15.7s**

The time calculated above is the maximum time taken to transfer the data from IBCard to IBDetector including discovery and connection times. However, during experiments the Ericsson Bluetooth module at the IBDetector end hardly took more than 2 seconds (avg.) to discover and connect to the IBCard's Bluetooth module, thus reducing the total time to 6.3 sec. RSA encryption is done before storing data on IBCard and decryption is done at the IBDetector's end so that the speed of the system is not limited by the card processor.

MANUFACTURABILITY AND MARKETABILITY

The system requires further development to meet the production requirements. This requires integration of Bluetooth with microcontroller-based Smart Cards. The power consumption of the Bluetooth radio and the battery life of the card is one of the important considerations. *Table 2* lists the specifications of a currently available Bluetooth chip, a microcontroller Smart Card, and long-lasting miniature battery that shows design is feasible. Additional implementation concerns should be addressed during later stages of product development.

Table 2: Specifications for System Components

Ericsson Bluetooth Implementation		Varta Li_Manganese Dioxide Battery (LPF 25)[6]	
Power Consumption (active)	1.0mW	Max. discharge current	5mA
Nominal operating voltage	1.62-2.75V	Nominal Voltage	3V
Idle mode Current	30µA	Dimensions:	
Transmit Current	3mA	Length	22mm
Size	3.2cm^{2}	Width	29mm
Symbol rate	1MSps	Height	0.4mm
Bit error rate	0.1%	Weight	0.5g
Projected Cost	\$5	Typical Capacity	25mAh
Schlumberger Cryptoflex Cards		Life expectancy (typical)	>2 yrs
Power Supply	2.7-5.5V		
Memory Capacity	8-32KB		

The rate at which research is going on and demand been rising, these three technologies do promises a better future. The continuing decrease in cost, size and power requirements and more acceptances of these technologies will make the proposed system more feasible and cheaper.

CONCLUSIONS

The Personal Identification and Security System based on Bluetooth, Biometrics and Smart card Technologies provide both convenience and security. The mobile, low power and low cost Smartcards are the ideal medium for storing the personal information, retaining the small sizes of the conventional paper-based I-cards. Biometrics guarantees authentication, this combined with the capabilities of the Bluetooth technology - small size, low power and no line-of-sight requirements, the system promises a convenient and secure tomorrow.

The usage of this system in disaster times is one of major application in area of digital identification other than the traditional ones of identification and verification. With user being provided the facility of granting permission to access confidential parameters the issue of Civil rights and identity theft has also been dealt with.

Acknowledgements

We thank *Schlumberger Measurement and Systems India Limited* for sponsoring up the project. We also thank *B. K. Wadhwan* and *Subraneel Bose*, Schlumberger Measurement and Systems India Limited for their comments. We thank *Abhishek Shankar*, *Shyam B. Raghubanshi* and *Prachi Agarwal* for their collaboration in this article.

References

1. George Lawton, “Biometrics: A New Era in Security”, *IEEE Computer*, Vol. 33, No. 8, pp 16-18, August 1998.
2. Lin Hong and Anil Jain, “Integrating Faces and Fingerprints for Personal Identification”, *IEEE transactions on Pattern Analysis and Machine Intelligence*, Vol. 20, No. 12, pp 1295-1307, December 1998.
3. Bluetooth White Paper 1.1, . AU-System, January 2000 10; http://137.132.153.41/bluetooth/papers/au_system.pdf
4. Michael Thieme, “Smart Cards and Biometrics – A Solution for human Services?”, *Biometrics in Human Services*, Vol. 4, Issue 2, March 2000; http://www.dss.state.ct.us/digital/news18/bhsug18.htm
5. Roger Cummings, “The Evolution of Information Assurance”, *IEEE Computer*, Vol. 35, No. 12, pp 65-72, December 2002.
6. Varta Li_Manganese Dioxide Battery (LPF 25) specifications; http://microbatteries.varta.com/MB_DATA/DOCUMENTS/DATA_SHEETS/DS6804.PDF