RFID with Bio-Smart Card in Linux

Suhas A Desai, *Research Student*

D. B. Kulkarni, *Assistant Professor*

Abstract-- **In this paper, we describe the integration of fingerprint template and RF smart card for clustered network, which is designed on Linux platform and Open source technology to obtain biometrics security. Combination of smart card and biometrics has achieved in two step authentication where smart card authentication is based on a Personal Identification Number (PIN) and the card holder is authenticated using the biometrics template stored in the smart card that is based on the fingerprint verification. The fingerprint verification has to be executed on central host server for security purposes. Protocol designed allows controlling entire parameters of smart security controller like PIN options, Reader delay, real-time clock, alarm option and cardholder access conditions.**

Index Terms—RFID, smart cards, biometrics security, Linux platform

1 INTRODUCTION

The RF Smart Card and card reader/writer were developed to handle payment transaction for public transportation systems. These contact less cards have security features, such as encrypted RF transmission mutual authentication, and security keys. The RF smart card has up to 16 separate sectors, which can be configured as purses or for general data storage. The first sector is typically used as a directory for the rest of the card, leaving 15 segments available for data or purses.

Each sector has two keys, called the A and B keys, allowing different access privileges to that sector. These key pairs can be designated as read and read/write, or decrement and increment/decrement .For example this would allow turnstile readers with the A key to only deduct value from a card sector, while smart card readers with the B keys could either add or subtract value .The card also has a 32-bit unique random number, which is permanently encoded into each chip by the chip manufacturer.

Public key infrastructure (PKI) based systems are used to construct a secure system that can achieve secure access conditions. They are consequently being used to carry keys and store personal information in applications such student identification systems.

The user validation could still be security-hole with assumption of private keys. Penetration rate of biometrics, which is referred to as the false match rate (FMR), can be statically controlled by decision parameter, and be depend on the user's senses of security.

Suhas A Desai, D. B. Kulkarni are with the Department of Computer Science and Engineering, Walchand College of Engineering, Sangli, MS, India-416415
Email: suhas_swan@yahoo.com, d_b_kulkarni@yahoo.com

2 ACCESS CONTROL SYSTEMS AND BIOMETRIC SMART CARD

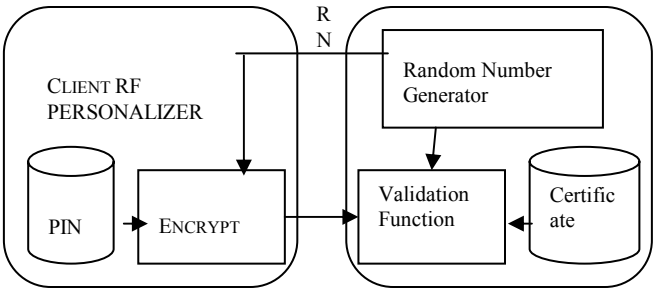


Figure 2.1 Access Control Client-Server Architecture

The client stores a user's certificate including a public and a private key that are issued by a certification authority in advance. A random number (RN) generated by the server is encrypted with the private key in the client, then the encrypted random number (ERN) is validated in the server with both CA's and the use's certificate.

In the case of embedding a fingerprint matching function into the server, the transmission of fingerprint images from the client to the server is required. This requirement means that other transmission protocols specialized for user validation must be added to the system. However, this is not desirable for standard entity authentication systems because of the prohibitive cost. Therefore, the matching function must be embedded in the client in this case. For a similar reason, the templates must be stored in the client. Although there are actually many choices of connection between fingerprint matching and entity authentication, activation of the user's private key or the encryption function depending on the result of the fingerprint matching is appropriate in consideration of matching junction and the template residing in the client.

Figure 2.2 shows the functional blocks of the client according to the above considerations. User's private key and the encryption function are embedded in the smart card.

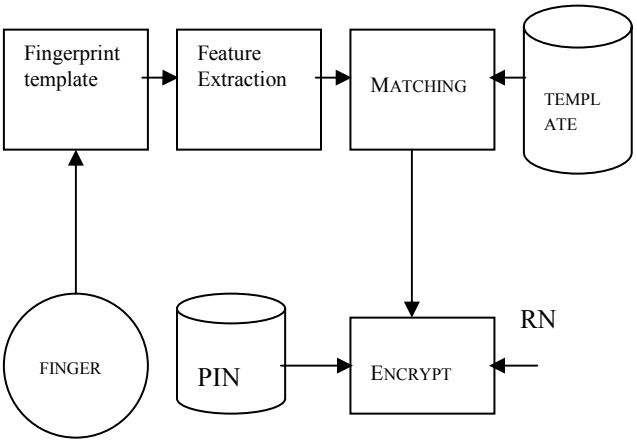


Figure 2.2 Functional blocks of the client

Figure 2.3 shows the proposed students ID identification system consisting of a smart card template and authentication functions. The card reader has a fingerprint scanner and a processor to capture fingerprints and to extract features of the fingerprints, respectively.

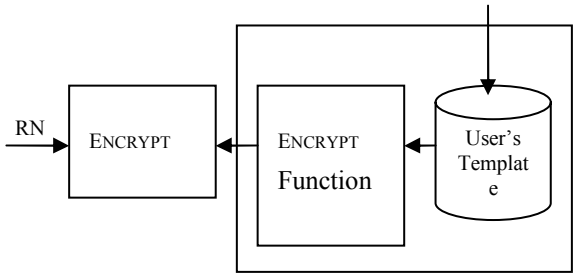


Figure 2.3 students ID card authentication system

Personalizer does not allow a backing of the fingerprint images and their features. The card reader also performs an encryption function, and thus data communication between the reader and the card are safeguarded against from any backing attempts. The matching function in the smart card executes a fingerprint matching function in the smart card execute a fingerprint matching between the features acquired by the reader and these stored in the user's template in the card. If a fingerprint is matched to the template, then the function unlocks the user's private key. Finally, the encryption functions execute the entity authentication based on the PKI.

3 CLUSTERED FINGERPRINT MATCHING THROUGH HOSTS

Figure 3.1 shows clustered network to distribute entire biometric template to verify and give results at central secure server. This server then send requests to access for authenticates to person. The fingerprint matching process is more important than the feature extraction process in the development of the proposed system, because the CPU in typical smart cards have low calculation power and the card dose not have enough memory space to execute the matching process. Therefore, a fingerprint-matching algorithm specialized for the CPU embedded in a smart card is required. Thus, we regarded the fingerprint matching process to be executed in the smart card as the first step of development. The fingerprint verification algorithm consisting of enrollment and verification processes. In the enrollment process, the fingerprint image captures by the scanner is enhanced, binaries, and thinned, and then the feature points (minutia) and the core of the fingerprint are extracted from the image. The coordinates of the feature points and the core, and small images around the feature points and the core, and small images around the feature points called "chip images", are stored into the template of the fingerprint. The chip images are also bit images that describes a bit per pixel.

In the verification process, the fingerprint image inputted for verification is enhanced and binaries by the same method of the enrollment, and then the core is extracted. After correcting the translation between the fingerprints image and the template, each small image stored in the template is a coordinate of the feature point. This process is called "chip matching". In the chip matching process, it is decided that the chip image is found on the fingerprint, as long as the number of the same bits between the chip and fingerprint images exceeds a threshold. The matching process can be executed quickly by performing a logical operation (XOR) and counting bits using a table. The fingerprint is considered verified if the number of the chip images found on the fingerprint is over a threshold. To embed the chip matching function into a smart card, smart card's shortage of memory space creates a bottleneck This limitation does not allow the storing of the entire fingerprint image in the memory at one time, Therefore, the developed chip matching scheme uses a partial image of the captured the fingerprint that is transmitted to the smart card then matched to the chip image in turn.

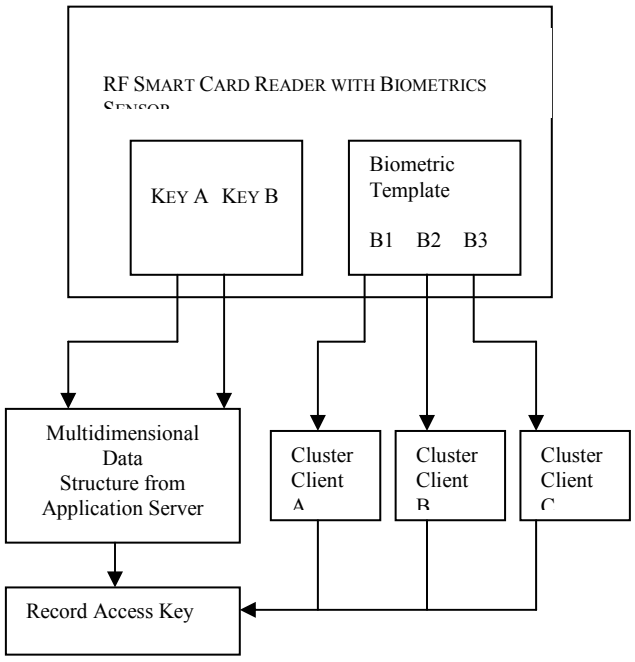


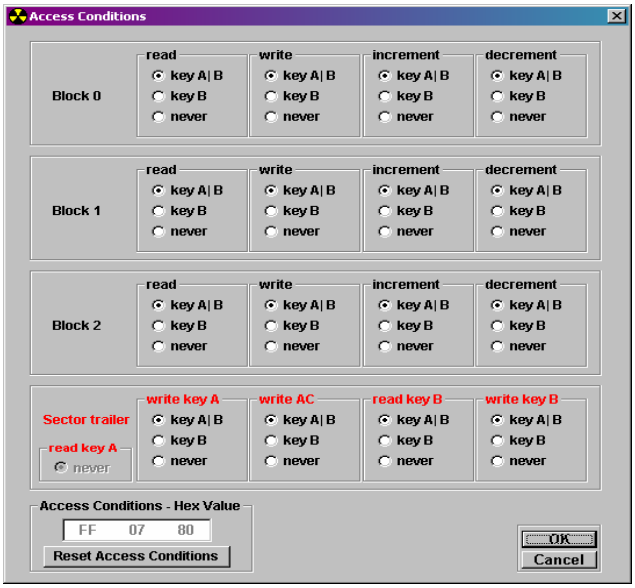
Figure 3.1 Clustered network to access control

4 ACCESS CONDITIONS AND CRYTPOGRAPHY

The card memory is organized as 8192 Bit EEPROM, which is split into 16 sectors with 4 blocks. One block consists of 16 bytes. The first block of the memory is reserved for manufacturer data like 32 bit serial number. This is a read only block. It is named as “Block 0”. Access conditions for the Data Blocks are defined in the Sector Trailers. According to these conditions data can be read, written, incremented, decremented, transferred or restored either with Key A, Key B or never. The RF Smart card consists of two types of Data Blocks: Read/write blocks, Value blocks.

4.1 Sector Trailer

The fourth block of any sector is the Sector Trailer. The Sector Trailer contains access Key A, an optional Key B and the access conditions for the four blocks of that sector. The typical access conditions of the RF smart card are as:



Above screen shows the default access conditions of a sector.

Important security issue is the cryptographic protection of biometric data. A PIN is a secret, but some biometric data are of public nature - such as fingerprints. The only possibility to avoid such an attack from the viewpoint of the smart card is the cryptographic protection of the biometric verification data.

In closed environments, the cryptographic protection may be achieved by using symmetric algorithms. In public environments, however, the usage of asymmetric algorithms with card verifiable certificates is appropriate. For performance reasons, asymmetric cryptography is not to be directly applied to biometric data.

5 CENTRAL SERVER HOST AND SMART CARD TEMPLATE

A biometric system can be used to control the access of users to determine places and/or services. Unfortunately, the user's template is a piece of sensible data that should be stored securely. Several systems exist nowadays that uses biometric identification. Some of these systems have the templates of all users stored in a secure central database. This leads to the necessity of apply an online communication from all the Point of Service (PoS) to that central database server. When the biometric identification is required, the system read the template from the smart card, and then performs the matching inside the host. This have two main weak points: the host should be highly protected against hacking and Trojans; and also, the services provided by the smart card, such as e-purse operations, cannot be secured biometrically. The main problem is the lack of an initial reference to sort the minutiae found. This lack makes it necessary to perform an alignment between the template stored and the feature vector obtained from the sample captured, and then, to convert both to polar coordinates.

6 LINUX BASED REULTS

1.Biometrics security can be obtained with protocol designing on Linux platform. This secure clustered protocol gave results for at a time 54-attendance queue within 3-second delay. Key-set and biometric template shows combination of PIN and fingerprint security with data uploading facility, cryptographic data transmission and accurate access control system on Linux network system. Open source technology with java comm. API’s gave better results for RF technology. However, the corresponding error tolerance ability will be weakened.

2.The results obtained show the possibility of integrating biometrics as a Card Holder Verification method, therefore, improving 73 percent user authentication in smart card based applications (automated Tea Vending Machine). This is a personal authentication model that uses fingerprint verification and the MULTOS card, and indicated framework of the general authentication based on the PKI with all clustered network-having MULTOS.

3.In the implemented system, the client personalizer is only interfaced between the smart card to the application server and only checks PIN. A Linux platform technology provides runtime environment to the proper transaction support for the reliable update of data.

4.Computational power of RF smart card depends on data retention of 10 years with write endurance 1,00,000 cycles and it is really small. In smart cards, initial clock should be at most of 5MHz (4MHz if using 3volt smart cards). This reduces greatly the computational speed, unless a clock multiplier is integrated in the processor die. But clock multipliers cannot be of any value, in order to give a clean and symmetric clock signal, and not creating RF signals that interfere with processor data movement.

5.The other inconvenience is the semi-duplex asynchronous serial transmission. Under typical conditions, the initial transfer rate is 9600bps, and, although it can be changed, it cannot be more than 115Kbps. Also, protocols used cannot exchange more than 255 bytes in a single transfer, so if the biometric sample is larger, more than one transfer should be used.

6.With all these considerations, restrictions that RF smart cards play over biometric security are:

- Biometric samples should be quite short. More than 512 bytes are not acceptable, due to RAM requirements and time lost in data communication.
- User template, though it has no restrictions in data communications (because it is only sent once, during the enrollment phase), should not be two large. As larger it is, more EEPROM will be used for its storage, and longer will be take in the matching algorithm.
- Fixed-point arithmetic operations should be reduced, and floating point ones must be avoided. If not, a mathematic coprocessor will be needed, increasing the die cost.

7 REFERENCES

[1] Moon, Y.S.; Ho, H.C.; Ng, K.L.; Wan, S.F.; Wong, S.T., "Collaborative fingerprint authentication by smart card and a trusted host", Electrical and Computer Engineering, 2000 Canadian Conference, Volume: 1,7-10 March 2000, Pages: 108 – 112.

[2] Sanchez-Reillo, R., "Smart card information and operations using biometrics", Aerospace and Electronic Systems Magazine, IEEE, Volume: 16, Issue: 4, April 2001, Pages: 3 – 6

[3] Yoichi Seto, "Development of personal authentication systems using fingerprint with smart cards and digital signature technologies", Control, Automation, Robotics and Vision, 2002. ICARCV 2002. 7th International Conference, Volume: 2, 2-5 Dec. 2002 ,Pages: 996 - 1001 vol.2

[4] Sanchez-Reillo, R.; Sanchez-Avila, C.; Mengibar-Pozo, L., "Microprocessor smart cards with fingerprint user authentication", Security Technology, 2002. Proceedings. 36th Annual 2002 International Carnahan Conference, 20-24 Oct. 2002,Pages: 46 – 49

[5] Toji, R.; Wada, Y.; Hirata, S.; Suzuki, K.,"A network-based platform for multi-application smart cards", Enterprise Distributed Object Computing Conference, 2001. EDOC '01. Proceedings. Fifth IEEE International, 4-7 Sept. 2001, Pages: 34 – 45

[6] Wen-Shenq Juang, "Efficient multi-server password authenticated key agreement using smart cards", Consumer Electronics, IEEE Transactions, Volume: 50, Issue: 1, Feb. 2004, Pages: 251 – 255