

# Secure Authentication Protocol with Biometrics in an M-Commerce Environment

Wan S. Yi<sup>1</sup>, Woong Go<sup>2</sup>, Dongho Won<sup>1</sup>, Jin Kwak<sup>2\*</sup>

<sup>1</sup> Information Security Group, Sungkyunkwan University,  
300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea  
{wsyi, dhwon}@security.re.kr

<sup>2</sup> Department of Information Security Engineering, Soonchunhyang University,  
646 Eupnae-ri, Shinchang-myun, Asan-si, Chungcheongnam-do, 336-745, Korea  
{wgo, jkwak}@sch.ac.kr

**Abstract.** Growth in the number of mobile device users and the market has led to the development of m-commerce. However, mobile devices have security issues, such as third party's illegal use of lost mobile devices or weaknesses in security. This paper analyzes an m-commerce system. We propose a secure authentication protocol with biometrics in an m-commerce environment.

**Keywords:** Biometrics, M-Commerce, Mobile Device, User Authentication

## 1 Introduction

Modern society offers convenience and efficiency to users through various devices. E-commerce has made great progress with anytime, anywhere access to e-commerce through mobile networks. In Korea, mobile devices started to diffuse in the late 1990s. 90% of households in the country now have a mobile device. As the range of services and products has increased, so has the number of users. M-commerce is superior to e-commerce in offering spatiotemporal access, due to the ubiquitous nature of mobile devices.

However, mobile devices have security issues. Security measures are lower than for PCs and have an increased risk of loss. A user utilizing m-commerce via a mobile device must apply a certificate stored in a smart chip. Thus, if the mobile device is lost, the smart chip also lost. This may give rise to abuse from malicious attackers. Thus, payment using mobile devices is burdensome to users.

This paper proposes a biometrics-based m-commerce protocol to increase security and circumvent problems from loss of mobile device loss. It also considers a secure payment system.

This remainder of this paper is organized as follows. Section 2 describes m-commerce. Section 3 describes a secure authentication protocol with biometrics in the

---

\* Prof. Jin Kwak, he is the corresponding author

m-commerce environment. Section 4 presents security and analyses efficiency. Section 5 concludes the paper.

## **2 M-Commerce**

There are many definitions for the term M-Commerce. Common to all definitions is that a terminal or mobile device is employed to communicate over a mobile telecommunication network. There are different views as to the purpose of this communication. Some definitions restrict m-commerce to transactions involving a monetary value, whereas other definitions generalize the term to services that involve communication, information, transaction, and entertainment. Summarizing, we define M-Commerce as using a mobile device for business transactions performed over a mobile telecommunication network. This optionally involves the transfer of monetary value [1].

### **2.1 Mobile Devices**

M-Commerce is not just about using mobile phones as end user devices. The following list gives an overview of different kinds of mobile devices, such as mobile phones, PDAs (Personal Digital Assistant), smart phones, laptops, and Earpieces (as part of a Personal Area Network).

Each mobile device has characteristics that influence its usability, such as

- Size and color of display
- Input device, availability of keyboard and mouse
- Memory and CPU processing power
- Network connectivity, bandwidth capacity
- Supported operating systems
- Availability of internal smart card reader( e.g., SIM card)

Depending on these factors, the services that the end user can receive differ considerably. Moreover, depending on the network technology used for transmission, the bandwidth capacity varies and influences the kind of services that the end user is able to receive.

### **2.2 Wireless Public Key Infrastructure**

This section describes WAP and ME as representative wireless internet protocols supporting a mobile device. It considers security technologies based on the wireless protocols and their issues.

Unlike a wired network, a wireless network has many restrictions. A mobile device does not have the same computational ability and storage capacity as a desktop computer. Wireless communication has lower transmission bandwidth than its wired

counterpart. Applying the wired Internet protocols to mobile phones has many problems, such as limitations in the screen size, computing power, and memory capacity. Wireless Internet technologies have been developed to overcome these restrictions of the wireless environment [2].

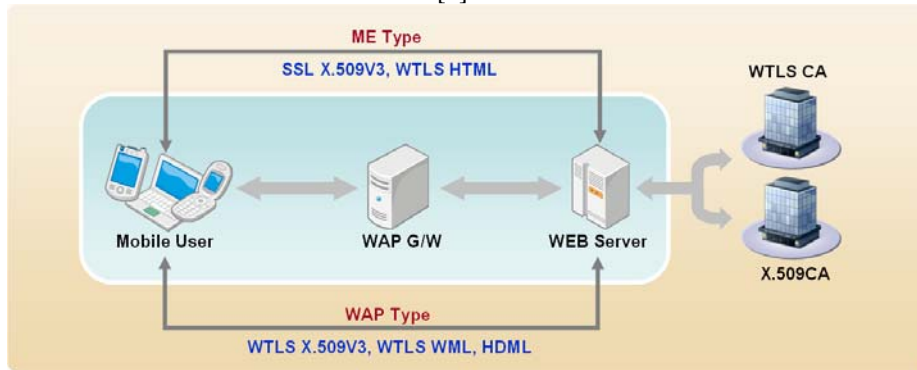


Fig. 1. WAP and ME in WPKI

**WAP Security.** In WAP 1.x, security service is provided by WTLS, equivalent to SSL of the wired Internet, as shown in Figure 2. WTLS is a security protocol developed based on the Internet Engineering Task Force (IETF)'s Transport Layer Security (TLS) in a manner suited to the wireless environment.

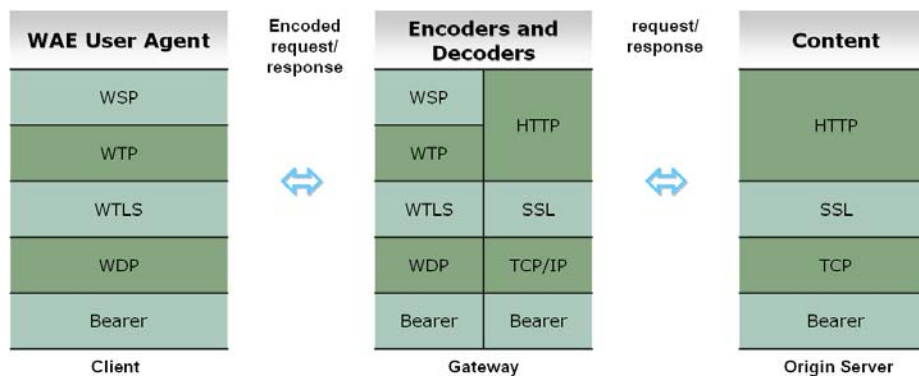
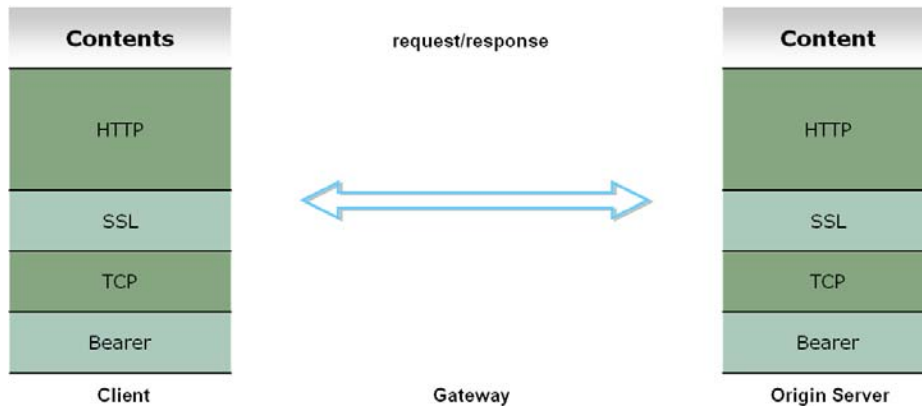


Fig. 2. WAP 1.x configuration

**ME Security.** Version 1.0 of ME does not have a secure protocol. However, a domestic security software company developed SSL 3.0 for mobile phones. It implemented it to ME, as shown in Figure 3. Additionally, SEED, the Korean standard block algorithm, was implemented.



**Fig. 3. ME configuration**

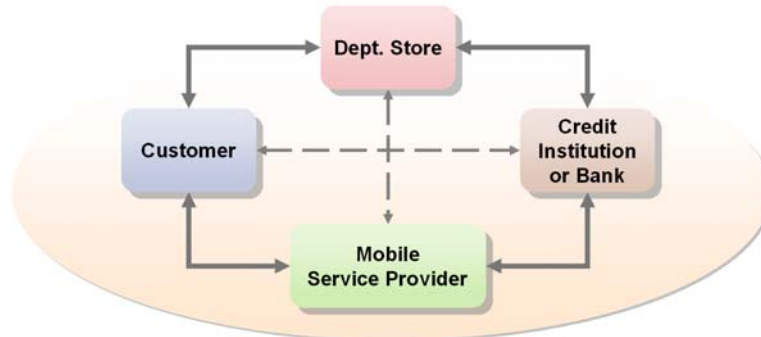
### 2.3 M-Commerce Value Chain

A range of different relationships need to be established in different the m-commerce transactions. These relationships will need to be explored in some detail to determine the types of problems that could occur in m-commerce. Different types of protection need to be established for different elements in the value chain. Figures 4 and 5 illustrate the different relationship types that could emerge. These involve a range of different relationships between different parties.



**Fig. 4. Relationships between the customer and the mobile services provider**

In Figure 4, a relationship exists between the customer and the mobile service provider. The provider supplies content, and bills the customer for the service. The mobile service provider has a separate relationship with a content provider. While the customer purchases content from a third party, this relationship is transparent and the only relationship that exists for a consumer is that with the mobile service provider [3].



**Fig. 5.** Relationship involving financial institutions

This figure depicts the relationship that a customer may have in conducting a more complex m-commerce transaction. In this case, the customer might have a relationship with the mobile service provider that enables the transaction to take place. The customer may have been required to establish a virtual bank account to purchase product. This handles the transactions that the customer makes, and payments for products etc. The customer will also have a relationship with the department store for the purchase of goods [3].

### **3 Proposed Secure Authentication Protocol with Biometrics in an M-Commerce Environment**

M-commerce, as described in this paper, is growing rapidly, due to mobile device diffusion and increase in transmission speed. Users can use various services with m-commerce, such as play games, see movies, and make payments.

The existing m-commerce must apply the certificate stored in a smart chip to make the payment. In this case, when the mobile device is lost, a malicious attacker may use it. If there is not a user authentication procedure reliability becomes an issue. Large fictitious payments may be attempted using the lost mobile device.

#### **3.1 The Risk of M-Commerce Environment**

M-commerce with a mobile device should apply a user certificate for authentication in the mobile device. The user should give a password to access and use the certificate. However, there are several security problems to store the user certificate in mobile device. These problems are as follows:

**The risk of loss.** If the user loses the certificate stored in the mobile device, a malicious attacker can pay for services or products using it. It inflicts financial harm to the user. M-commerce using a mobile device can use a traffic card or credit card. Therefore, the malicious attacker can buy services or products without authentication. Thus, losing a mobile device with an embedded certificate causes a risk.

**Vulnerable of security by low computation power.** Most mobile devices have lower computational ability than a PC. That is, security strength in m-commerce using a mobile device is lower than for e-commerce using a PC. Thus, the m-commerce authentication method is WPKI, a lightweight PKI used in the wired network for the wireless network.

**Wireless Risk.** M-commerce information is transmitted through the wireless environment using the mobile device. Malicious users may eavesdrop on information transmitted wirelessly. Most transmitted information is encrypted, but a malicious attacker may decrypt it using a chosen-plaintext attack or analysis of alphabet frequency.

This paper proposes a secure authentication protocol using biometrics in an m-commerce environment to solve these problems.

### 3.2 Proposed Protocol

An advantage of the protocol proposed in this paper is that it can use a variety of biometric information. Mobile devices offer different hardware systems, of which, one is a camera that can recognize the user's face. Some mobile devices have a fingerprint recognition interface. Accordingly, users can use a recognition interface without needing an additional device. This is advantageous to both users and vendors. This can increase the mobile device's efficiency and the user's convenience.

Through the development of technology, the mobile device can recognize various biometrics proposed in the protocol later.



**Fig. 6.** Fingerprint mobile phone ('L' company) and facial recognition mobile phone ('S' company)

The following are forms of biometric information.

**Fingerprints.** The pattern of ridges and valleys on an individual's fingertip is unique. Fingerprints are unique for each finger of a person, including identical twins. One of the most commercial available biometric technologies, fingerprint recognition devices for PC access are widely available from many different vendors at a low cost. With these devices, the user no longer needs to type a password. Fingerprint systems can also be used in identification mode.

**Speaker Recognition.** Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy and learned behavioral patterns. This incorporation of learned patterns into the voice templates has earned speaker recognition its classification as a "behavioral biometric." Speaker recognition systems employ three styles of spoken input: text-dependent, text-prompted and text-independent. Most speaker verification applications use text-dependent input. This involves selection and enrollment of one or more voice passwords. Text-prompted input is used when there is the possibility of imposters.

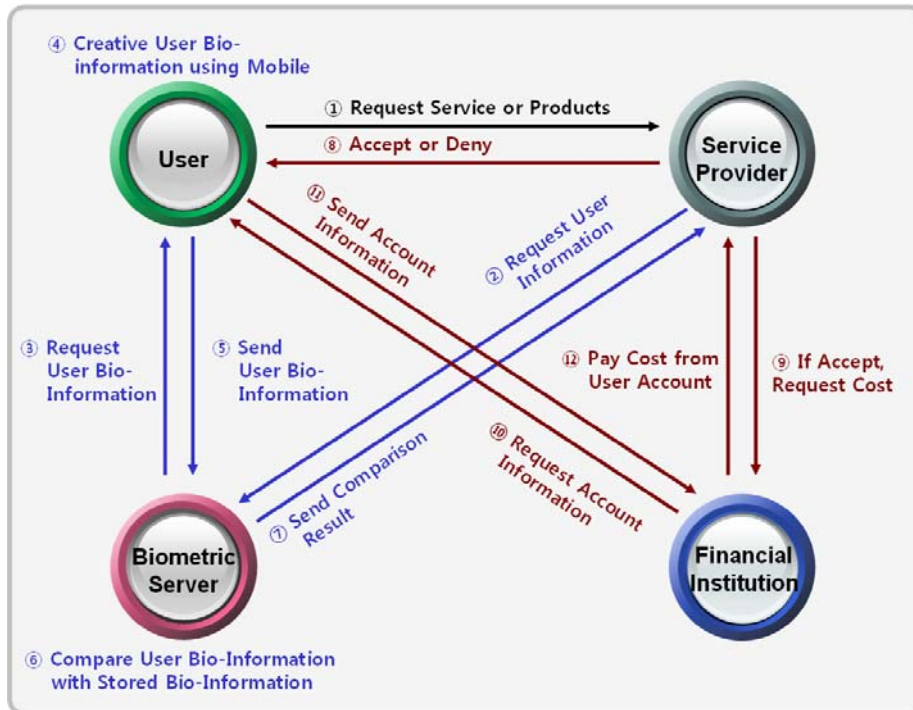
**Face Recognition.** The identification of a person by their facial image can be done in a number of different ways, such as capturing an image of the face in the visible spectrum using a camera or using the infrared patterns of facial heat emission. Facial recognition in visible light typically models key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image that do not change over time. They avoid superficial features, such as facial expressions or hair.

**Iris Recognition.** This recognition method uses the iris of the eye. The iris is the colored area that surrounds the pupil. Iris patterns are unique. The iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. The technology works well in both verification and identification modes (in systems performing one-to-many searches in a database). The technology is not intrusive. It does not require physical contact with a scanner. Iris recognition has been demonstrated to work with individuals from different ethnic groups and nationalities [5].

Users can choose whether or not to participate in m-commerce service. Thus, participation is voluntary and information collection can be considered unobtrusive. Hence, if you want to use m-commerce, you must do the following.

- You must have a mobile device that can recognize a biometric feature.
- You must store your personal biometric information with a trusted institution.
- The user can choose the biometric information they want.(e.g. fingerprint, Iris)

Figure 7 is a simple depiction of the proposed protocol. Blue arrows represent procedure authentication protocols. Red arrows are procedure payment protocols.



**Fig. 7.** Proposed Biometrics Based M-Commerce System

In Figure 7, we don't discuss about key exchange protocols between all entities for simplify procedure. Proposed biometrics based m-commerce system on the supposition that all of entities are trusted institutions.

- ① User requests services or products from the Service Provider (SP).
- ② The SP requests user's identification from the Biometric Server (BS).
- ③ The BS requests biometric information from the User
- ④ User inputs biometric information using the mobile device (The same biometric information they first selected when they registered)
- ⑤ The biometric information is sent to the BS.
- ⑥ The BS compares the received biometric information to the stored biometric information.
- ⑦ The BS sends the result of the comparison to the User.
- ⑧ The SP accepts or denies the User based on the compared result.
- ⑨ If User authentication is complete, the SP requests the cost from the Financial Institution (FI).
- ⑩ The FI notifies the user of this, and requests account information.
- ⑪ The User sends account information to the FI.
- ⑫ The FI pays the cost to the SP

Figure 8 details the proposed protocol.

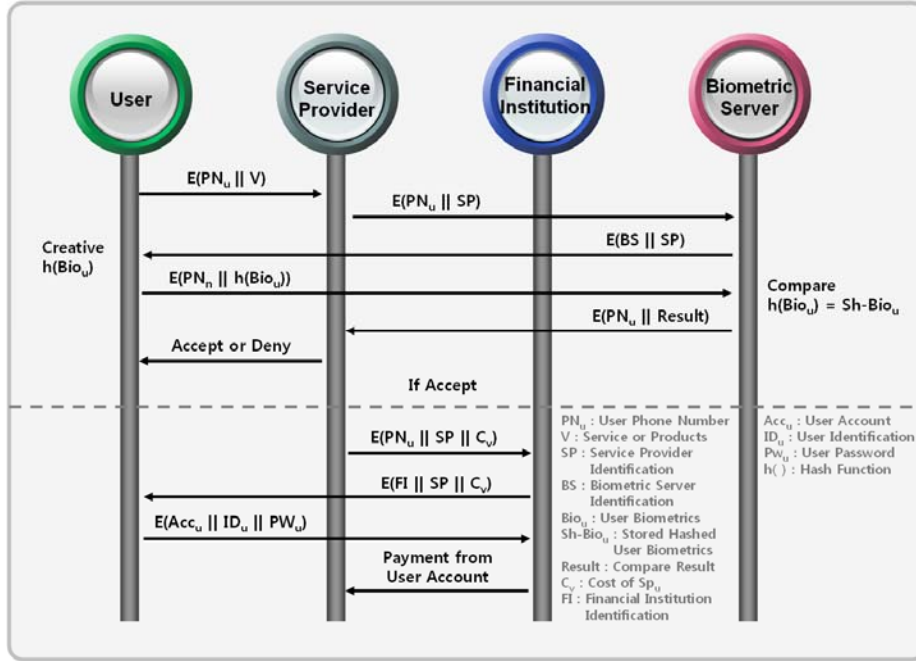


Fig. 8. Proposed Secure Authentication Protocol with Biometrics

The encryption method in this protocol uses ECC (Elliptic Curve Cryptosystem). ECC is a public key cryptosystem. Therefore, anyone can encrypt and decrypt information using the public key and secret key.

This protocol shows all user authentication and payment procedures. This procedure shows more simply protocol than other m-commerce protocol.

The user sends the mobile phone number and service or product information to the SP to utilize the service or products.

$$E(PN_u || V) \quad (1)$$

The SP sends his identification and user's mobile phone number to the BS, and requests verification of the user's identity. The BS verifies the SP identification.

$$E(PN_u || V) \quad (2)$$

The BS requests biometric information for authentication from the user by sending his identification and SP identification. The user verifies the BS identification whether or not s/he first registered with that institution. The SP identification is used

to validate the SP whether or not s/he requested products or services from that provider.

$$E(\text{BS} \parallel \text{SP}) \quad (3)$$

The user captures and hashes biometric information using the mobile device, and sends it with the mobile phone number to the BS.

$$\begin{aligned} \text{Compare } h(\text{Bio}_u) &= \text{Sh-Bio}_u \\ E(\text{PN}_u \parallel h(\text{Bio}_u)) & \end{aligned} \quad (4)$$

The BS compares the received and stored hashed biometric information to verify the right user. The BS sends the result of the comparison with the user's phone number to the SP. The user's phone number is used to ascertain whose biometric information is to be checked.

$$E(\text{PN}_u \parallel \text{Result}) \quad (5)$$

The SP accepts or denies service to the user as a result of the comparison. If user authentication is complete, the SP sends the User phone number, the SP identification, and the cost to the FI. This step ends user authentication and initiates the payment procedure.

$$\begin{aligned} &\text{Accept or Deny User} \\ &\text{If Accept, send} \\ &E(\text{PN}_u \parallel \text{SP} \parallel C_v) \end{aligned} \quad (6)$$

The FI sends the FI identification, the SP identification, and the cost to the User to request account information and user authentication. This step will prevent illegal cost claims from malicious attackers.

$$E(\text{FI} \parallel \text{SP} \parallel C_v) \quad (7)$$

The User verifies the received information from the FI, and sends account information, ID, and password.

$$E(\text{ACC}_u \parallel \text{ID}_u \parallel \text{PW}_u) \quad (8)$$

After user verification, the FI pays the cost to the SP.

## 4 Security and Efficiency Analysis

The proposed authentication protocol in m-commerce focuses on improving security. Therefore, this protocol lacks efficiency compared to existing m-commerce authentication methods. However, since financial transactions take place in m-commerce, improving security through user authentication is more important than efficiency.

**Table 1. Comparison of Security and Efficiency**

	The Risk of Loss	Security Authentication Factor	Wireless Security	Efficiency Computational Time
Existing M-Commerce Authentication Protocol	Low.	Middle	Middle	High
Proposed M-Commerce Authentication Protocol	High	High	Middle	Low

- Security – The Risk of Loss

This factor concerns the security issue of mobile device loss. The certificate is lost with the mobile device in the existing m-commerce environment. This engenders illegal use by a malicious attacker. Thus, security is set at a low level (low is the lowest level in this comparison). The proposed protocol sets the level at high, because it does not store authentication information in the mobile device.

- Security – Authentication Factor

This factor concerns the security issue of the authentication factor. The proposed protocol uses biometric information, the most unique of authentication factors, for user authentication. It presents the highest level of security. Therefore, the security level is high. The existing m-commerce authentication protocol uses a PKI-based certificate for user authentication. The certificate represents a middle level relative to biometrics.

- Security– Wireless Security

This factor concerns the security issue of the wireless network. In this paper, we propose using the WPKI protocol used by existing m-commerce. Therefore, they represent the same level. However, wireless networks have more problems than wired networks. Thus, security is considered to be at the middle level.

- Efficiency – Computational Time

This factor concerns the efficiency of computational time. The protocol proposed in this paper uses biometric information using a camera or fingerprint interface. However, this procedure is more complex than for existing m-commerce. Existing m-commerce just inputs a password to access information, but the proposed m-commerce protocol inputs biometric information and processes this.

#### **4.1 Suitable for Mobile Environments**

The protocol, as describes in this paper, designed for authentication with user biometrics. It use ECC at cryptosystem for suitable for mobile environments, and it can make up for the computational ability in the mobile device. Besides, secure transmission is guaranteed through cryptosystem.

This protocol has the Biometric Server for user authentication with biometrics. The Biometric Server is connected and transmission with other entities, it provides more secure authentication system in mobile environments.

### **5 Conclusion**

M-commerce is growing rapidly as the number of users with mobile devices increases. M-commerce is superior to e-commerce using a PC in terms of spatiotemporal availability. M-commerce with a mobile device must apply a certificate stored in a smart chip. Therefore, if the mobile device is lost, the smart chip also lost. This can enable abuse from a malicious attacker, since an inserted smart chip always can trigger the payment. Thus, this paper examines m-commerce systems and biometric information. We proposed a biometric-based m-commerce protocol to solve these issues.

The proposed protocol is expected to be able to increase m-commerce security. The user can access services and products in a securer environment.

### **References**

1. Tiwari, R., Buse, S., Herstatt, C., : Customer on the Move – Strategic Implications of Mobile Banking for Banks and Financial Enterprises. In: “CEC/EEE 2006, Proceedings of The 8<sup>th</sup> IEEE International Conference on E-Commerce Technology, pp.522-529. San Francisco (2006)
2. Anckar, B. and D’Incau D., : Value-Added Services in Mobile Commerce - An Analytical Framework and Empirical Findings from a National Consumer Survey : World Wide Web, <http://csdl.computer.org/comp/proceedings/hicss/2002/1435/03/14350086b.pdf>
3. Khodawandi, D., Poustchi, K. and Wiedemann, D.G., : Mobile Commerce – Anwendungen und Perspektiven :pp.42-57 Augsburg (2003)
4. Pankanti. S., Bolle. R. M., Jain. A., : Biometrics The Future of Identification :, IEEE Computer Magazine. (2000)
5. S. Prabhakar, S. Pankanti, A.. K. Jain, : Biometric Recognition Security and Privacy Concerns : IEEE Security & Privacy, pp.33-42. (2003)