INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 5, Issue 3 JUNE 2016

BIOMETRIC BASED USER AUTHENTICATION USING SMART CARD

P.RAMESH [1], Y.BALAGANGADHAR REDDY [2]

[1] P.Ramesh, M.Tech student, Dept Of ECE, Priyadashini Institute Of Technology, Ramachandrapuram, Tirupathi, Jntu Anatapur, A.P., India.

[2] Y.Balagangadhar Reddy, Assistant Professor, Dept Of ECE, Priyadashini Institute Of Technology, Ramachandrapuram, Tirupathi, Jntu Anatapur, A.P., India.

Abstract: Remote user authentication is one of the major issues in the rapid growing internet era. In this paper we propose a biometric based remote user authentication scheme using smart cards. The existing methods failed to be safe in remote user authentication as the secret values in either end of the communication could be guessed by the intruder. In our scheme we introduce an addition security at the user side as an extra once by which the intruders will be unable to guess the users secret data. Hence our proposed scheme proves to provide a strong authentication and non-repudiation even in an insecure communication by sending and receiving messages with timestamps.

***Key words**: Microcontroller, Finger Print Module, USB Camera, MIC, LCD Display.*

I. Introduction

The rapid development of Internet technologies legitimate users access the remote resources over the insecure communication channel by the use of user identity and password. User authentication is an essential security mechanism for remote system to assure one communicating party that validates the corresponding party. Biometric authentication is a procedure to identify the individuals based on biological and behavioral traits(finger print ,iris, face, palm print, retina, hand geometry, voice, signature and gait).Biometric authentication are reliable and secure than traditional password based authentication. Using biometric keys in the user authentication process have many advantages. Bio metric keys cannot be lost or forgotten. Bio metric keys are very difficult to copy or share. Bio metric keys are extremely hard to forge or distribute. Bio metric keys cannot be guessed easily. Bio metric keys are not easily to break. Hardware-based selective unlocking schemes have been proposed previously. These include: Blocker Tag, RFID Enhancer Proxy, RFID Guardian, and Vibrate-to-Unlock. A Faraday cage can also be used to prevent an RFID tag from responding promiscuously by shielding its transmission. Cryptographic protocols, Distance bounding protocols, Context-aware selective unlocking, Motion detection has been proposed as another selective unlocking scheme. All of these approaches, however, require the users to carry an auxiliary device.

II. The Hardware System

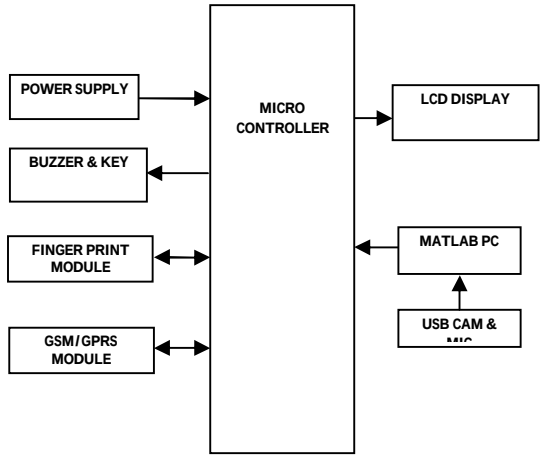
Micro controller: This section forms the control unit of the whole project. This section basically consists of a Microcontroller with its associated circuitry like Crystal with capacitors, Reset circuitry, Pull up resistors (if needed) and so on. The Microcontroller forms the heart of the project because it controls the

devices being interfaced and communicates with the devices according to the program being written.

ARM7TDMI: ARM is the abbreviation of Advanced RISC Machines, it is the name of a class of processors, and is the name of a kind technology too. The RISC instruction set, and related decode mechanism are much simpler than those of Complex Instruction Set Computer (CISC) designs.

Liquid-crystal display: Lcd is a flat panel display, electronic visual display that uses the light modulation properties of liquid crystals. Liquid crystals do not emit light directly. LCDs are available to display arbitrary images or fixed images which can be displayed or hidden, such as preset words, digits, and 7-segment displays as in a digital clock.

III. Design of Proposed Hardware System



In this paper, we have first reviewed the recently proposed scheme and then shown that their scheme is vulnerable to the known session-specific temporary information attack and thus, their scheme fails to prevent reply attack and cannot provide strong user anonymity. Also, we have demonstrated the drawbacks in existing method while distributing the static authentication parameters and with the wrong password entry. To withstand these drawbacks, we have proposed a novel and efficient multi-server authentication protocol using biometric-based fingerprint detection and image and voice recognisation. When all these parameters are authorized the transactions are done by using GPRS server.

Buzzer: A buzzer or beeper is a signaling device, usually electronic, typically used in automobiles, household appliances such as a microwave ovens, & game shows. The word "buzzer" comes from the rasping noise that buzzers made when they were electromechanical devices, operated from stepped-down AC line voltage at 50 or 60 cycles. Other sounds commonly used to indicate that a button has been pressed are a ring or a beep.

The "Piezoelectric sound components" introduced herein operate on an innovative principle utilizing natural oscillation of piezoelectric ceramics. These buzzers are offered in lightweight compact sizes from the smallest diameter of 12mm to large Piezo electric sounders. Today, piezoelectric sound components are used in many ways such as home appliances, OA equipment, audio equipment telephones, etc. And they are applied widely, for example, in alarms, speakers, telephone ringers, receivers, transmitters, beep sounds, etc.

Fig 1: Types of Buzzers

Fingerprint module:

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. FIM 30 has functions of fingerprint enrollment, identification, partial and entire deletion and reset in a single board, it does not require connection with a separate PC, thereby offering convenient development environment.

Features

- On-line and off-line fingerprint identification incorporated
- Identification rate 1:1 and 1:N; FAR: 1/100.000 y FRR: 1/1.000
- Algorithm and high hardness optical sensor
- It provides high recognition ratio even to small size, wet, dry, calloused fingerprint.
- Fast acquisition of difficult finger types under virtually any condition.
- Memory capacity for 100 fingerprints
- Memory events: up to 2,000 authentications
- Access host can be protected by fingerprint or password
- It offers convenient development environment.
- Two communication ports: RS-232 or host (on-line applications)
- ASCII protocol
- Supply voltage: 5V
- Small size and robust durability, it has longer life span.

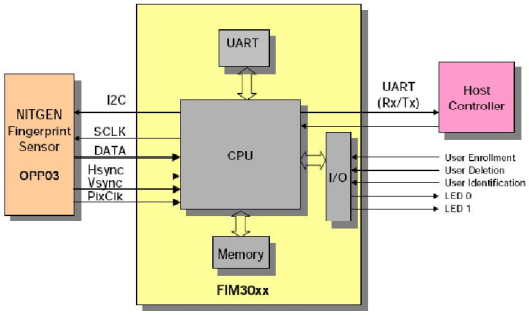


Fig 2: Finger print module

Webcam:

"Webcam" refers to the technology generally; the first part of the term ("web-") is often replaced with a word describing what can be viewed with the camera, such as a net cam or street cam. Webcams are video capturing devices connected to computers or computer networks, often using USB or, if they connect to networks, Ethernet or Wi-Fi. They are well-known for low manufacturing costs and flexible applications. **Video capture** is the process of converting an analog video signal—such as that produced by a video camera or DVD player—to digital form. The resulting digital data are referred to as a digital video stream, or more often, simply video stream. This is in contrast with screen casting, in which previously digitized video is captured while displayed on a digital monitor

Webcams typically include a lens, an image sensor, and some support electronics. Various lenses are available, the most common being a plastic lens that can be screwed in and out to set the camera's focus. Fixed focus lenses, which have no provision for adjustment, are also available. Image sensors can be CMOS or CCD, the former being dominant for low-cost cameras, but CCD cameras do not necessarily outperform CMOS-based cameras in the low cost price range. Consumer webcams are usually VGA resolution with a frame rate of 30 frames per second. Higher resolutions, in mega pixels, are available and higher frame rates are starting to appear.

Fig 3: Webcam

The video capture process involves several processing steps. First the analog video signal is digitized by an analog-to-digital converter to produce a raw, digital data stream. In the case of composite video, the luminance and chrominance are then separated. Next, the chrominance is demodulated to produce color difference video data. At this point, the data may be modified so as to adjust brightness, contrast, saturation and hue. Finally, the data is transformed by a color space converter to generate data in conformance with any of several color space standards, such as RGB and YCbCr. Together, these steps constituted video decoding, because they "decode" an analog video format such as NTSC orPAL.

Support electronics are present to read the image from the sensor and transmit it to the host computer. The camera pictured to the right, for example, uses a Sonix SN9C101 to transmit its image over USB. Some cameras - such as mobile phone cameras - use a CMOS sensor with supporting electronics.

Features:

- Smallest wireless video & audio camera
- Wireless transmission and reception
- High sensitivity
- Easy installation & operation
- Easy to conceat
- Light weight
- Low power consumption
- Small size

Specifications:

- Output frequency: 900MHZ 1200MHZ
- Output power: 50mW 200mW
- Power supply: DC +6~12v
- Distance covered: 10m

GPRS:

GPRS (General Packet Radio Service) is a packet based communication service for mobile devices that allows data to be sent and received across a mobile telephone network. GPRS is a step towards 3G and is often referred to as 2.5G. Here are some key benefits of GPRS .GPRS usage is typically charged based on volume of data transferred, contrasting with circuit switched data, which is usually billed per minute of

connection time. Usage above the bundle cap is either charged per megabyte or disallowed.

GPRS is a best-effort service, implying variable throughput and latency that depend on the number of other users sharing the service concurrently, as opposed to circuit switching, where a certain quality of service (QoS) is guaranteed during the connection. In 2G systems, GPRS provides data rates of 56–114 kbit/second.[3] 2G cellular technology combined with GPRS is sometimes described as *2.5G*, that is, a technology between the second (2G) and third (3G) generations of mobile telephony.[4] It provides moderate-speed data transfer, by using unused time division multiple access (TDMA) channels in, for example, the GSM system. GPRS is integrated into GSM Release 97 and newer releases. As mentioned earlier GPRS is not a completely separate network to GSM. Many of the devices such as the base transceiver stations and base transceiver station controllers are still used. Often devices need to be upgraded be it software, hardware or both. When deploying GPRS many of the software changes can be made remotely. There are however two new functional elements which play a major role in how GPRS works. The Serving GPRS Support Node (SGSN) and the Gateway GPRS support node (GGSN).

Fig 4: GPRS module

IV. CONCLUSION

In this paper a new biometric based user authentication scheme using smart card has been proposed. The proposed scheme improves in order to provide strong authentication and non-repudiation and defend against the replay attacks, man in middle attacks, and stolen verification attacks. The proposed scheme updates the password freely without the knowledge of registration center. Our scheme has double security protection mechanism where message are transmitted over an insecure channel. When compared with other schemes our scheme enhances the security in terms of security goals.

V. REFERENCES

[1] Lamport.L,"Password authentication with in secure communication", Communications of the ACM, Vol 24, No 11,1981, pp. 770-772.

[2] Li C-T, Hwang M S, "An online biometrics based secret sharing scheme for multiparty cryptosystem using smartcards", Journal of Innovative Computing Information and Control ", Vol. 6, No. 5, 2010a, pp. 2181-2188.

[3] Chun-Ta Li, Min-Shiang Hwang, "An efficient biometrics based remote user authentication scheme using smart cards", Journal of Network and Computer Applications",Vol. 33, No. 1, 2010b, pp. 1-5.

[4] Li X, Niu J-W, Ma J., Wang W-D, Liu C.L "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart

cards", Journal of Network and Computer Applications, Vol. 34, No 1, 2011,pp.73-79.

[5] A.K.Das "Analysis and improvement on an efficient biometric based remote user authentication scheme using smart cards", IET Information Security", Vol 5, No 3, 2011,pp. 145-151.

[6] Sandeep K Sood, Anil K Sarie and KuldipSingh, "A Secure dynamic identity based authentication protocol for multiserver environment", Journal of Network and Computer Applications",Vol. 34, No. 2, 2011, pp. 609-618