Smart Card System with High Authentication Technology

Jamuna.P [1]
Assistant Professor
Department of EEE,
ravikumarjamuna@gmail.com,

Sivasangari.G [2]
PG Scholar,
M.E (Embedded system Technologies)
sivasangari92@gmail.com,

Tamilselvan.K [3]
PG Scholar,
M.E (Embedded system Technologies)
tamilselvankesavan@yahoo.com

Nandha Engineering College (Autonomous), Erode, Tamilnadu, India.

Abstract- The Paper develops the Automatic Teller Machines process. Now a day's usage of banking sector is essential to the people with a help of ATM Cards. In the Proposed systems multiple ATM cards are merge into a one card is smart Card. ARM7 plays a vital source and execute a certain task in a Efficient Process. The Ethernet standards comprise several wiring and signaling variants of the OSI physical layer in use with Ethernet. Host computer is user side. Packets are transfer server to domain with a help connection establishment.LED display improve the clarity of color contrast. Efficiency of These display improve the quality. And reduce the power consumption. Vein authentication system is a type of security system.

Keywords- RTOS, ARM7, LED, RS232, ATM.

I.INTRODUCTION

Embedded system is a special computer system that bases on computer technology, focuses on application, software and hardware customizable, suitable for the strict requirement of application system on function, reliability, cost, volume and power. It is widely used in military, civil electronics, household appliances and consumption electronic products in recent years. But most of the embedded systems are used independently at current stage, RS-232 and RS-485 are the most commonly used technologies to deal with the communication between multiple microprocessors in industrial control fields and has the disadvantages such as low transmission rate, limited coverage, relatively less communication protocols, etc., which cause it very difficult to perform flexible remote access and management. The Ethernet (IEEE 802.3) is the most mature and widely used LAN technology, connecting the embedded device to the network device such as Hub, switch thus realizing a flexible real time control and monitoring has already become an inevitable development trend of embedded technology. In this paper, the design and implementation process of a monitoring system based on ARM7. ARM 7 LPC2378 development kit with DP83848H module, are connected using a crossover Ethernet cable RJ 45. On the transmission side, user-entered data is compiled into an IEEE 802.3 frame; on the reception side, data is extracted from the frame and displayed through the network analyzer.

II.RTOS

A real-time operating system (RTOS) is an operating system (OS) intended to serve real-time application requests. It must be able to process data as it comes in, typically without buffering delays. Processing time requirements (including any OS delay) are measured in tenths of seconds or shorter. A key characteristic of an RTOS is the level of its consistency concerning the amount of time it takes to accept and complete an application's task; the variability is jitter. A hard real-time operating system has less jitter than a soft real-time operating system. The chief design goal is not high throughput, but rather a guarantee of a soft or hard performance category. An RTOS that can usually or generally meet a deadline is a soft real-time OS, but if it can meet a deadline deterministically it is a hard real-time OS.An RTOS has an advanced algorithm for scheduling. Scheduler flexibility enables a wider, computer-system orchestration of process priorities, but a real-time OS is more frequently dedicated to a narrow set of applications. Key factors in a real-time OS are minimal interrupt latency and minimal thread switching latency; a real-time OS is valued more for how quickly or how predictably it can respond than for the amount of work it can perform in a given period of time. Here micro controller operated version2 is used.

III. SMART CARD

1.1 Functions

SCard Begin Transaction: This function starts a transaction, waiting for the completion of all other transactions before it begins.

SCard Cancel: This function terminates all outstanding actions within a specific resource manager context.

SCard Connect: This function establishes a connection, using a specific resource manager context, between the calling application and a smart card contained by a specific reader.

SCard Control: This function gives you direct control of the reader. You can call it any time after a successful call to SCard Connect and before a successful call to SCard Disconnect.

SCard Free Memory: This function frees memory that has been returned from the resource manager using the SCARD_AUTOALLOCATE length designator.

SCard Disconnect: This function terminates a connection previously opened between the calling application and a smart card in the target reader.

SCard End Transaction: This function completes a previously declared transaction, enabling other applications to resume interactions with the card.

SCard Establish Context: This function establishes the resource manager context (the scope) within which database operations is performed.

SCard Get Status Change: This function blocks execution until the current availability of the cards in a specific set of readers changes.

SCard Introduce Reader: This function introduces a new name for an existing smart card reader. Smart card readers are automatically introduced to the system.

SCard Introduce Card Type : This function introduces a smart card to the smart card subsystem for the active user by adding it to the smart card database.

SCard List Readers : This function searches the readers listed in the register Reader States parameter for a card with an Automatic Terminal Recognition (ATR) string that matches one of the card names specified in message Cards, returning immediately with the result.

SCard Release Context: This function closes an established resource manager context, freeing any resources allocated under that context, including SCARDHANDLE objects and memory allocated using the SCARD_AUTOALLOCATE length designator.

SCard Set Attrib: This function sets the specified reader attribute for the specified handle.

SCard Is Valid Context : This function determines whether a smart card context handle is valid.

SCard Transmit : This function sends a service request to the smart card and expects to receive data back from the card.

1.2 Processor Interfacing ARM

The LTC1755/LTC1756 universal Smart Card interfaces are fully compliant with ISO 7816-3 and EMV specifications. The parts provide the smallest and simplest interface circuits between a host microcontroller and general purpose Smart Cards. An internal charge pump DC/DC converter delivers regulated 3V or 5V to the Smart Card, while on-chip level shifters allow connection to a low voltage controller. All Smart Card contacts are rated for 10kV ESD, eliminating the need for external ESD protection devices.

Input voltage may range from 2.7V to 6.0V, allowing direct connection to a battery. Internal soft-start mitigates start-up problems that may result when the input power is provided by another regulator. Multiple devices may be paralleled and connected to a single controller for multi-card applications.

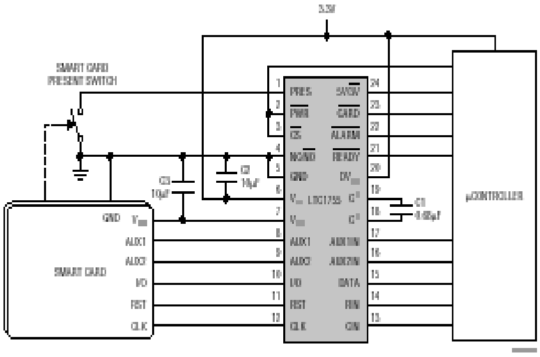


Fig 1.2: Interfacing

Battery life is maximized by 60µA operating current and 1µA shutdown current. The narrow SSOP packages minimize PCB area for compact portable systems. Extensive applications are Handheld Payment Terminals Pay Telephones Key Chain Readers Smart Card Readers

1.3 Features

Fully ISO 7816-3 and EMV Compliant (Including Auxiliary I/O Pins). Buck-Boost Charge Pump Generates 3V or 5V.2.7V to 6.0V Input Voltage Range (LTC1755).Very Low Operating Current 60µA.10kV ESD on All Smart Card Pins. Dynamic Pull-Ups Deliver Fast Signal Rise Times. Soft-Start Limits Inrush Current at Turn On. 3V - 5V Signal Level Translators. Shutdown Current: <1µA. Short-Circuit and Over temperature Protected. Alarm Output Indicates Fault Condition. Multiple Devices May Be Paralleled for Multicar Applications (LTC1755). Available in 16- and 24-Pin SSOP Packages Network Protocols.

The Internet protocol suite is the networking model and a set of communications protocols used for the Internet and similar networks. It is commonly known as TCP/IP, because it’s most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), were the first networking protocols defined in this standard. It is occasionally known as the DOD model, because the development of the networking model was funded by DARPA, an agency of the United States Department of Defense.

TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. This functionality has been organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved.

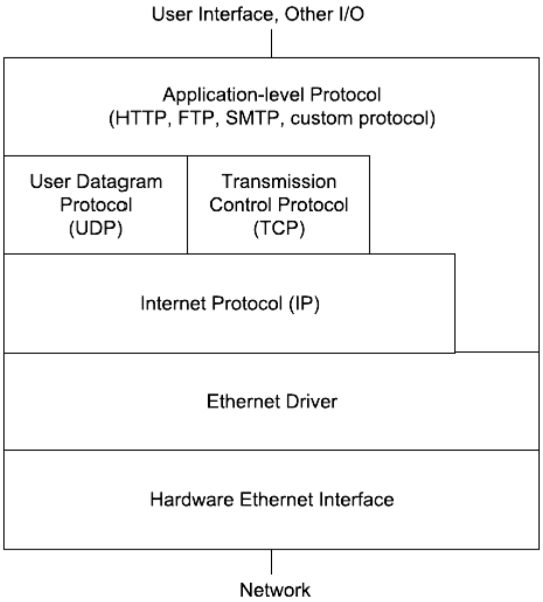

User Interface, Other I/O
Application-level Protocol
(HTTP, FTP, SMTP, custom protocol)
User Datagram Protocol (UDP)
Transmission Control Protocol (TCP)
Internet Protocol (IP)
Ethernet Driver
Hardware Ethernet Interface
Network

Fig 1.3: Network Layer

From lowest to highest, the layers are the link layer, containing communication technologies for a single network segment (link), the internet layer, connecting independent networks, thus establishing internetworking, the transport layer handling process-to-process communication, and the application layer, which interfaces to the user and provides support services.

External smartcard pins	**STM320518 -EVAL**	**Function**
CLK	USART1_ CK: PA08	Smartcard clock: alternate function push-pull
IO	USART1_T X: PA09	IO serial data: alternate function open drain
RST	PB.15	Reset to card: output push-pull
Vcc	PC.13	Supply voltage: output push-pull
OFF	PA.11	Smartcard detect: input floating
3/5 V	PA.12	3 V or 5 V: output push-pull

Definition: IP (Internet Protocol) is the primary network protocol used on the Internet, developed in the 1970s. On the Internet and many other networks, IP is often used together with the Transport Control Protocol (TCP) and referred to interchangeably as TCP/IP

Definition: HTTP - the Hypertext Transfer Protocol - provides a standard for Web browsers and servers to communicate. The definition of HTTP is a technical specification of a network protocol that software must implement.

Definition: FTP allows you to transfer files between two computers on the Internet. FTP is a simple network protocol based on Internet Protocol and also a term used when referring to the process of copying files when using FTP technology.

1.3.1 Ethernet

Ethernet is a family of computer networking technologies for local area networks (LANs). Ethernet was commercially introduced in 1980 and standardized in 1983 as IEEE 802.3.Ethernet has largely replaced competing wired LAN technologies such as token ring, FDDI, and ARCNET.

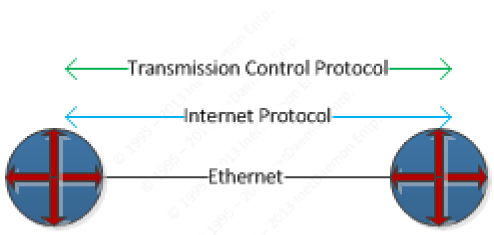


Fig 1.3.1: Ethernet

The Ethernet standards comprise several wiring and signaling variants of the OSI physical layer in use with Ethernet. The original 10BASE5 Ethernet used coaxial cable as a shared medium. Later the coaxial cables were replaced with twisted pair and fiber optic links in conjunction with hubs or switches. Data rates were periodically increased from the original 10 megabits per second to 100 gigabits per second.

Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses and error-checking data so that damaged data can be detected and re-transmitted. As per the OSI model

Ethernet provides services up to and including the data link layer.

1.3.2 Advanced networking

Simple switched Ethernet networks, while a great improvement over repeater-based Ethernet, suffer from single points of failure, attacks that trick switches or hosts into sending data to a machine even if it is not intended for it, scalability and security issues with regard to broadcast.

Advanced networking features in switches and routers combat these issues through means including spanning-tree protocol to maintain the active links of the network as a tree while allowing physical loops for redundancy, port security and protection features such as MAC lock down and broadcast radiation filtering, virtual LANs to keep different classes of users separate while using the same physical infrastructure, multilayer switching to route between different classes and link aggregation to add bandwidth to overloaded links and to provide some measure of redundancy.

IEEE 802.1aq (shortest path bridging) includes the use of the protocols to allow larger networks with shortest path routes between devices. In 2012, it was stated by David Allan and Nigel Bragg, in 802.1aq Shortest Path Bridging Design and Evolution: The Architect's Perspective that shortest path bridging is one of the most significant enhancements.

Separate from the underlying transmission techniques, 802.11 networks have a variety of security mechanisms. The original 802.11 specifications defined a simple security protocol called WEP. This protocol uses a fixed pre-shared key and the RC4 cryptographic cipher to encode data transmitted on a network. Stations must all agree on the fixed key in order to communicate. This scheme was shown to be easily broken and is now rarely used except to discourage transient users from joining networks. Current security practice is given by the IEEE® 802.11i specification that defines new cryptographic ciphers and an additional protocol to authenticate stations to an access point and exchange keys for data communication. Cryptographic keys are periodically refreshed and there are mechanisms for detecting and countering intrusion attempts. Another security protocol specification commonly used in wireless networks is termed WPA, which was a precursor to 802.11i. WPA specifies a subset of the requirements found in 802.11i and is designed for implementation on legacy hardware. Specifically, WPA requires only the TKIP cipher that is derived from the original WEP cipher. 802.11i permits use of TKIP but also requires support for a stronger cipher, AES-CCM, for encrypting data. The AES cipher was not required in WPA because it was deemed too computationally costly to be implemented on legacy hardware.

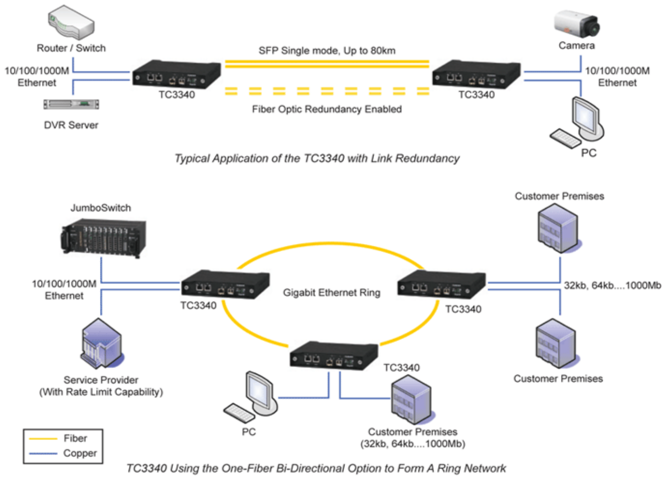

Router / Switch
10/100/1000M Ethernet
DVR Server
TC3340
SFP Single mode, Up to 80km
Fiber Optic Redundancy Enabled
TC3340
Camera
10/100/1000M Ethernet
PC
Typical Application of the TC3340 with Link Redundancy
JumboSwitch
10/100/1000M Ethernet
TC3340
Gigabit Ethernet Ring
TC3340
Customer Premises
32kb, 64kb....1000Mb
Service Provider (With Rate Limit Capability)
TC3340
Customer Premises
PC
Customer Premises (32kb, 64kb....1000Mb)
Fiber
Copper
TC3340 Using the One-Fiber Bi-Directional Option to Form A Ring Network

Fig 1.3.2: Working Block

1.4 Host Computer

A network host is a computer connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network. A network host is a network node that is assigned a network layer address. Computers participating in networks that use the Internet Protocol Suite may also be called IP hosts. Specifically, computers participating in the Internet are called Internet hosts, sometimes Internet nodes. Internet hosts and other IP hosts have one or more IP addresses assigned to their network interfaces. The addresses are configured either manually by an administrator, automatically at start-up by means of the Dynamic Host Configuration Protocol (DHCP), or by stateless address auto configuration methods.

1.5 *LED Display*

An LED display is a flat panel display, which uses an array of light-emitting diodes as a video display. An LED panel is a small display, or a component of a larger display. They are typically used outdoors in store signs and billboards, and in recent years have also become commonly used in destination signs on public transport vehicles or even as part of transparent glass area. LED panels are sometimes used as form of lighting, for the purpose of general illumination, task lighting, or even stage lighting rather than display.

Suitable locations for large display panels are identified by factors such as line of sight, local authority planning requirements if the installation is to become semi-permanent, vehicular access trucks carrying the screen, truck-mounted screens, or cranes, cable runs for power and video accounting for both distance and health and safety requirements, power, suitability of the ground for the location of the screen.

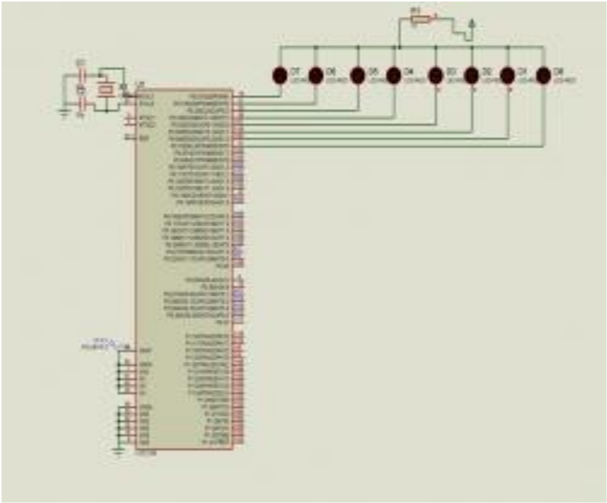


Fig: 1.5 LED display interface with arm processor using proteus simulator

1.6 *RS 232*

In telecommunications, RS-232 is the traditional name for a series of standards for serial binary single-ended data and control signals connecting between DTE (data terminal equipment) and DCE (data circuit-terminating equipment, originally defined as data communication equipment. It is commonly used in computer serial ports. The standard defines the electrical characteristics and timing of signals, the meaning of signals, and the physical size and pin out of connectors. The current version of the standard is TIA-232-F Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange, issued in 1997.

An RS-232 serial port was once a standard feature of a personal computer, used for connections to modems, printers, mice, data storage, uninterruptible power supplies, and other peripheral devices. However, the low transmission speed, large voltage swing, and large standard connectors motivated development of the Universal Serial Bus, which has displaced RS-232 from most of its peripheral interface roles. Many modern personal computers have no RS-232 ports and must use either an external USB-to-RS-232 converter or an internal expansion card with one or more serial ports to connect to RS-232 peripherals.

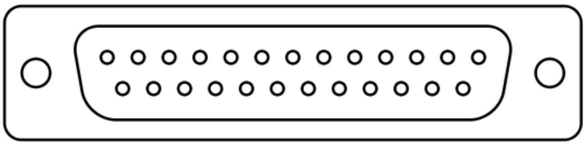


Fig 1.6: RS232

1.7 Keypad

A keypad is a set of buttons arranged in a block or "pad" which usually bear digits, symbols and usually a complete set of alphabetical letters. If it mostly contains numbers then it can also be called a numeric keypad. Keypads are found on many alphanumeric keyboards and on other devices such as calculators, push-button telephones, combination locks, and digital door locks, which require mainly numeric input.

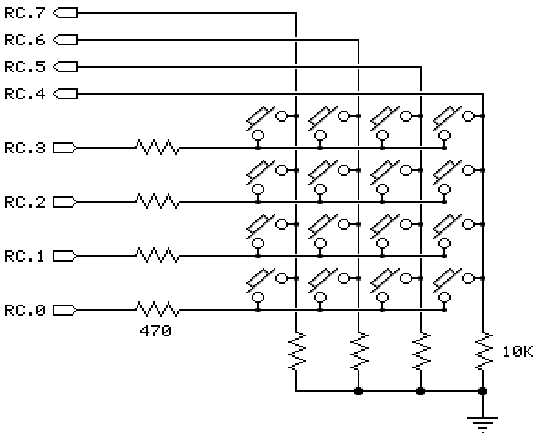


Fig 1.7: Keypad Interfacing

IV.ARM 7TDMI

The ARM architectures are reduced instruction set computer instruction set architectures, such as the currently marketed 64-bit ARMv8 and 32-bit ARMv7 and ARMv6 developed by British company ARM Holdings, who have designed and licensed a family of computer processors that use this instruction. This generation introduced the Thumb 16-bit instruction set providing improved code density compared to previous designs. The most widely used ARM7 designs implement the ARMv4T architecture, but some implement ARMv3 or ARMv5TEJ. All these designs use a Von Neumann architecture, thus the few versions comprising a cache do not separate data and instruction caches.

Some ARM7 cores are obsolete. One historically significant model, the ARM7DI is notable for having introduced JTAG based on-chip debugging;

the preceding ARM6 cores did not support it. The "D" represented a JTAG TAP for debugging; the "I" denoted an ICE Breaker debug module supporting hardware breakpoints and watch points, and letting the system be stalled for debugging. Subsequent cores included and enhanced this support.

It is a versatile processor designed for mobile devices and other low power electronics. This processor architecture is capable of up to 130 MIPS on a typical 0.13 µm process. The ARM7TDMI processor core implements ARM architecturev4T. The processor supports both 32-bit and 16-bit instructions via the ARM and Thumb instruction sets.

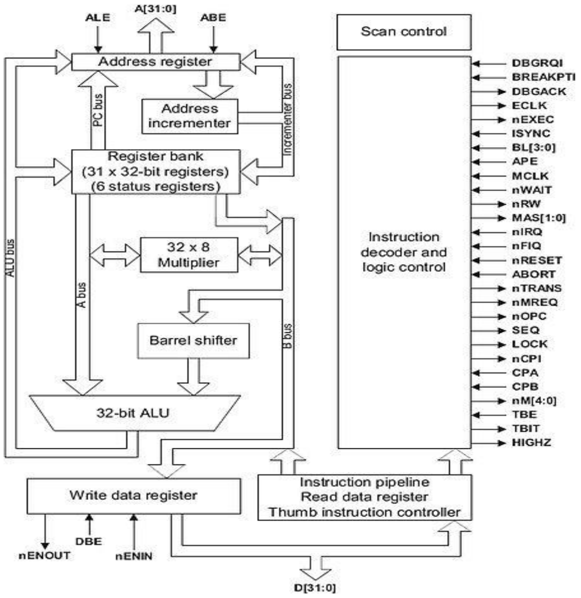


Fig 4: Block Diagram of ARM7

4.1ARM features

ARM Stands for Advanced RISC Machine ARM is a family of instruction set architectures for computer processors based on a Reduced Instruction Set Computing (RISC) architecture developed by British Company ARM Holdings. It is available in 32-bit or 64 bit.ARMv1First version of ARM processor.26-bit addressing, no multiply coprocessor. ARMv2, ARM2, First commercial chip. Included 32-bit result multiplies instructions. It Have a advanced Version of a Coprocessor support.

Smart card enters into the automatic teller machines. It will ask the security code. That time scanner will scan our vein access to open the account. it shown the multiple bank names. Then open a account efficiently by selection. With a help of Ethernet it displays the details in the display of Host computer. Energy alarm used difficult situations.

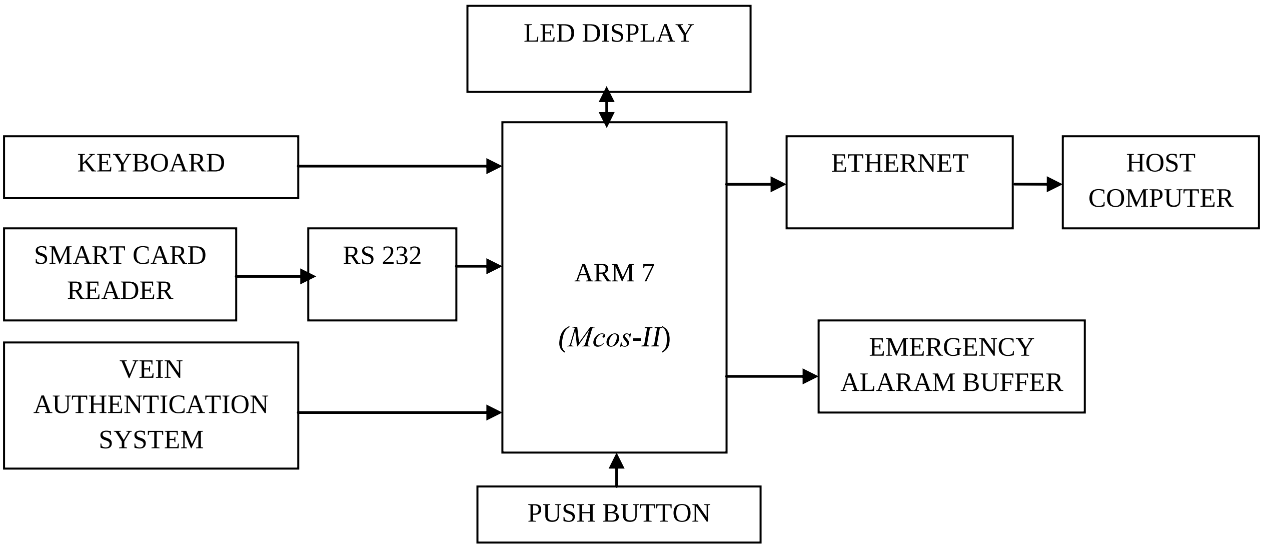


Fig 1: Block Diagram of a Smart Card System with Vein Authentication System

V.VEIN AUTHENTICATION SYSTEM

Finger vein recognition is a method of biometric authentication that uses pattern-recognition techniques based on images of human finger vein patterns beneath the skin's surface. Finger vein recognition is one of many forms of biometrics used to identify individuals and verify their identity Security.

Palm Vein Authentication Work flow-An individual inserts a smart card into the sensor device and holds her hand over the reader. The vein pattern is instantly captured using a completely safe near-infrared light. The reader converts the image into an encrypted biometric template and compares it against the template on the smart card (1 to 1 matching) or those in the database (1 to N matching).

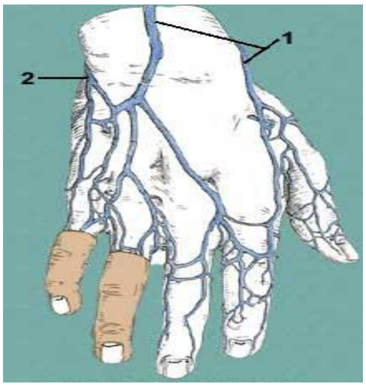
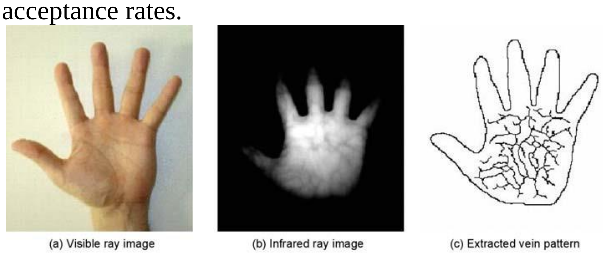


Fig 5: Vein of human hand

5.1Image Processing

The feature extraction approach is to use unique topological structure from the hand vein minutiae using Delaunay triangulation. A minutiae Mi can be represented by its position and type, *i.e*. Mi = (pi, qi, mi) where (pi, qi) denotes the position and mi denotes the type of minutiae (vein bifurcation or endings). The idea is to extract meaningful minutiae groups, *i.e*., triplets or triangles, from the hand vein map to achieve rotation and translation invariant representation of the local information. Given a minutiae triangle, we separately compute three lengths Lambda 1, Lamda2, and Lambda3. Then all the sides of triangle are sorted to avoid considering all possible orders of same lengths.

Accuracy and Reliability – Uniqueness and complexity of vein patterns, together with advanced authentication algorithms, ensure unsurpassed accuracy. Field test results show exceptionally low FTE (failure to enroll) rates, recognition attempt duration less than iris recognition, and near-zero false rejection and false acceptance rates.



(a) Visible ray image (b) Infrared ray image (c) Extracted vein pattern

Fig 5.1: Scanned Images from scanner

Security – Vein patterns are internal and unexposed, making them almost impossible to duplicate or forge. Images are converted into encrypted biometric templates at the sensor level, preventing misuse of the actual image.

Contactless – Hygienic, non-invasive, "no touch" technology enables use when hands are dirty, wet or even wearing some types of latex gloves.

Cost-Effective – Attractively priced while saving you the huge potential costs of malpractice litigation, privacy violations, etc. provides a high level of security at a Reasonable cost.

Usability – Compact form factor provides greater flexibility and ease of implementation in a variety of security applications. Application areas for palm vein technology are it supports variety of banking scenarios:

5.2Removing Noise

Once the extracted triplets are matched, using the criteria in equation, the matching scores are assigned. The score assignment scheme is hierarchical and assigns higher scores to more likely true matches. If two triplets having three bifurcation points are matched then there is higher probability that they corresponds to the same user vein map. Therefore such matches are assigned higher scores. However, those matching triplets formed due to three vein endings

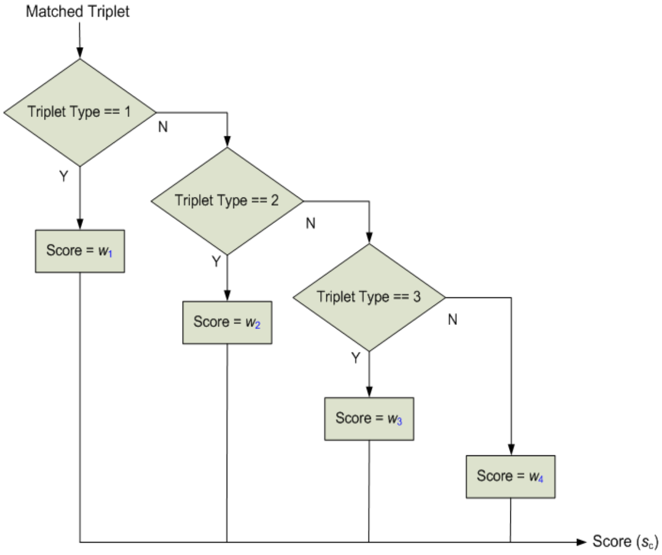


Fig 5.2: Flow Diagram

5.3 Data Analysis

The blood ensures that more incident infrared illumination changes its path in blood than in the surrounding tissue. It is scattering rather than absorption that dominates and results in the darker appearance of dorsal vein patterns. The figure 5.2 shows representation of Veins profiles along the direction perpendicular to their length. It can be observed from this figure that these vein profiles are quite noisy and do not have any ideal step edge to distinguish from the background. Although these intensity patterns varies from vein to vein, their average profile can be approximated as Gaussian. The widths of these vein profiles are found in the range of 30-50 pixels.

VI. CONCLUSION

Multiple bank accounts will maintain in a single bank account. That must be also in single smart card. Rs232 make a connection among hardware’s. ARM7 plays a efficient task to operate. LED display improves the quality. The edge point of vein patterns can be detected by locating zero crossings of second derivative gray level profiles. However, the derivative filters are very sensitive to the accompanying noise (fig.5.1.1) Therefore it is judicious to employ some pre-processing, such as averaging, to reduce the effect of noise. This two-step process (Laplacian of Gaussian) was found to be quite effective for the localization of venous structure in the acquired hand vein images.

References

[1] K.Tamilselvan “SD Card Based Data logging and retrieval for microcontrollers are using μcos-II” International journal for Engineering Research and Technology November 2013.

[2] Ajay Kumar, K. Venkata Prathyusha “Personal Authentication using Hand Vein Triangulation and Knuckle Shape” IEEE Transactions on Image Processing, September, 2009

[3] Sharvari B.Bhosale “network controlled monitoring system using arm 7” [IJESAT] international journal of engineering science & advanced technology Volume-2, Issue-3, June 2012

[4] Hui Chen “Resistance-temperature Characteristic Measurement System for Automotive Temperature Sensor Based on μcos-Ⅱ” International Conference on Information Science and Technology March 26-28, 2011 Nanjing, Jiangsu, China

[5] J. J. Labrosse, μcos-II: the Real Time Kernel. USA: CMP Books, 2002, pp. 179 – 198

[6] free scale semiconductor “Smart Card Operation Using Free scale Microcontrollers” 2/2012

[7] Rekha George, Dr. Varghese Paul “Design of ARM based Surveillance System with Ethernet interface” IOSR Journal of Electronics & Communication Engineering (IOSR-JECE) ISSN(e) : 2278-1684 ISSN(p)

[8] B. Srinivas Raj and G. Srinivas Babu, “ Design of Web based Remote Embedded Monitoring system**”,**
International Journal of Technology And Engineering System (IJTES): Jan –March 2011- Vol.2.No.2.