A Constraint-based Biometric Scheme on ATM and Swiping Machine

Mr V Manoj Kumar[1], Saravana Kumar T[2], Lokesh D[3], Pradeep Divakar R[4]
[1, 2, 3, 4] Department of Information Technology
[1]Assistant Professor, Saranathan College of Engineering
[2, 3, 4]Students, Saranathan College of Engineering

Abstract- *Report on a new approach for enhancing security and privacy in certain biometric applications. Show that location awareness can be used by biometric and back-end servers for defending against unauthorized reading and relay attacks on fingerprint systems. On the user side, design a location-aware selective unlocking mechanism. On the server side, Biometrics and GSM -Based Multi-Server Authentication Protocol design a verification scheme that allows a bank server to decide whether to approve or deny a payment transaction and detect a specific type of relay attack involving malicious readers. The premise of our work is a current technological advancement that can enable biometric with low-cost (GSM) sensing capabilities. Unlike prior research on this subject, our defenses do not rely on auxiliary devices or require any explicit user involvement.*

I. INTRODUCTION

The rapid development of the wireless communication networks and e-commerce applications, such as e-banking and transaction-oriented services, there is a growing demand to protect the user credentials privacy. In the recent couple of decades, more and more transactions for the mobile devices have been implemented on the Internet or wireless networks due to the portability property of mobile devices, such as laptops, smart cards and smart phones.

As a result, the user revocation and re-registration with the same identity is identified as fundamental security functionality for the smart card-based authentication schemes and they are

1) **SK-security:** An authentication scheme should guarantee the security of the session key, called the session key security (SK-security), in the following two cases:

(i) The leakage of session key or session-specific temporary information will have no effects on the security of other sessions.

(ii) The leakage of the crucial long-term secrets, such as the private keys of users or servers, which are used across the multiple sessions, will not necessarily compromise the secret information from all past sessions, known as the perfect forward secrecy.

2) **User credentials privacy:** It ensures that *A* cannot derive a user credentials, such as authentication parameter, user password and identity.

3) **Secure mutual authentication:** It ensures that an authentication scheme must provide the secure mutual authentication with the presence of the shared secret credentials.

II. COMPONENTS REQUIRED

2.1 Microcontroller 8051:

A microcontroller (also microcontroller unit, MCU or µC) is a small computer on a single integrated circuit consisting of a relatively simple CPU combined with support functions such as a crystal oscillator, timers, watchdog timer, serial and analog I/O etc. either Program memory in the form of NOR flash or OTP ROM is also often included on chip, as well as a typically small amount of RAM. Microcontrollers are designed for small or dedicated applications.

2.2 IR Sensor:

There is an obstacle, the green indicator light on the circuit board. The detection distance is 2 ~ 30cm and the detection angle is 35 °.The comparator chip is LM393. The circuit required to make an IR sensor consists of two parts; the emitter circuit and the receiver circuit. The emitter is simply an IR LED (Light Emitting Diode) and the detector is simply an IR photodiode which is sensitive to IR light of the same wavelength as that emitted by the IR LED. When IR light falls on the photodiode, its resistance and correspondingly, its output voltage, change in proportion to the magnitude of the IR light received. This is the underlying principle of working of the IR sensor.

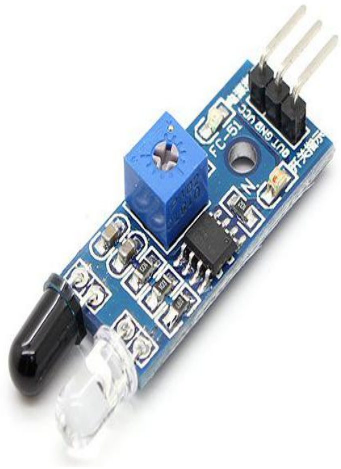

Fig 2.1 IR Sensor

2.3 GSM: GSM (Global System for Mobile communications: originally from *Group Special Mobile*) is the most popular standard for mobile phones in the world. Its promoter, the GSM Association, estimates that 80% of the global mobile market uses the standard. GSM is used by over 3 billion people across more than 212 countries and territories. Its ubiquity makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world. GSM differs from its predecessors in that both signaling and speech channels are digital, and thus is considered a *second generation* (2G) mobile phone system. This has also meant that data communication was easy to build into the system. GSM EDGE is a 3G version of the protocol.

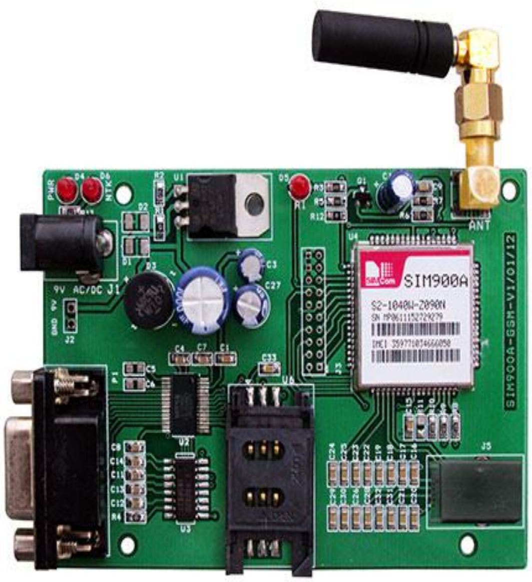

Fig 2.2 GSM Modem

2.4 ADC: ADC unit is used to convert the physical values from our sensors into digital values. It has 8 channels so that, we can connect 8 sensors at the time. But in PIC controller we have inbuilt ADC .If we are using AT8051 controller we have to interface it externally. The ADC0808, ADC0809 data acquisition component is a monolithic CMOS device with an 8-bit analog-to-digital converter, 8-channel multiplexer and microprocessor compatible control logic. The 8-bit A/D converter uses successive approximation as the conversion technique.

2.5 LCD DISPLAY: A liquid crystal display (LCD) is a thin, flat panel used for electronically displaying information such as text, images, and moving pictures. Its uses include monitors for computers, televisions, instrument panels, and other devices ranging from aircraft cockpit displays, to every-day consumer devices such as video players, gaming devices, clocks, watches, calculators, and telephones. Among its major features are its lightweight construction, its portability, and its ability to be produced in much larger screen sizes than are practical for the construction of cathode ray tube (CRT) display technology. Its low electrical power consumption enables it to be used in battery-powered electronic equipment.

2.6 FINGER PRINT SCANNER: Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity.

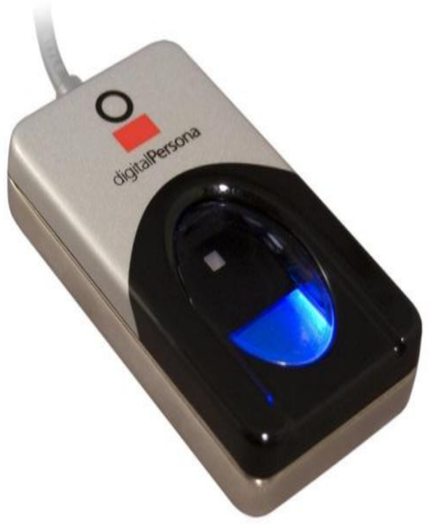

Fig 2.3 FINGER PRINT SCANNER

Fingerprint Scanner uses advanced CMOS sensor technology and precise optical system to deliver a high quality fingerprint image.

III. BLOCK DIAGRAM

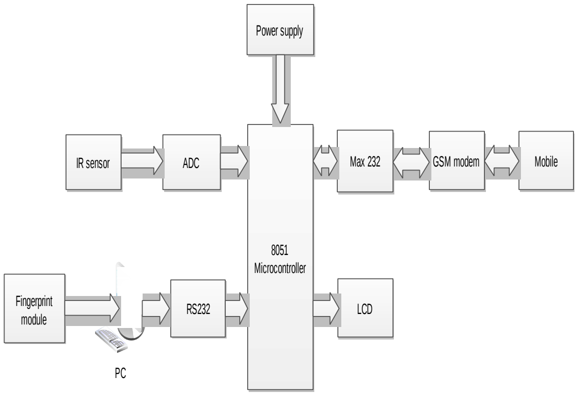

Fig 3.1 BLOCK DIAGRAM

This ATM Management Project adding some applications gives extra features to the customers. In This project we have used AT89c51 microcontroller, SIMMCOM GSM module, KEIL IDE tool, 2x16 LCD display. Initially the ATM module gets the password from the user mobile and it matches with the initial password. If it matches, then an ATM module allows the use entering the Amount. Otherwise ATM module will informs the bank that wrong user trying to access the bank. If the users entered the amount, ATM module sends this amount to the authority user mobile and waits for the ACK message from the Authority mobile.

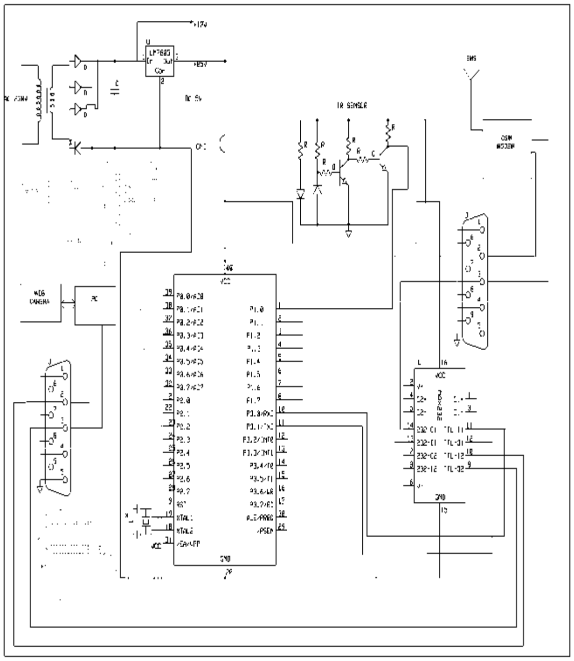

Fig 3.2 CIRCUIT DIAGRAM

If the ACK message is OK, then Process will be successfully completed. Otherwise it will inform the bank and also users Mobile that wrong user trying to Access the bank.

IV. CONCLUSION

Proposed He-Wang's 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, have demonstrated the drawbacks in He-Wang's scheme while distributing the static authentication parameters and with the wrong password entry. To withstand these drawbacks, proposed an efficient multi-server authentication protocol using biometric-based smart card and ECC. Shown that our scheme is secure and provides more functionalities as compared to He-Wang's scheme. Using the BAN logic proved that our scheme provides secure authentication through the formal security analysis. Simulated our scheme for the formal security verification using the widely-accepted AVISPA tool, and shown that our scheme is secure. In addition, through the informal security analysis, shown that our scheme is secure against various known attacks. Our scheme thus provides high security along with low communication cost, computational cost, and offers a variety of features.

REFERENCES

[1] M. O. Onyesolu and I. M. Ezeani, "ATM security using fingerprint biometric identifier: An investigative study," International Journal of Advanced Computer Science and Applications, vol. 3, no. 4, pp. 68-72, 2012.

[2] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMSFOR VIDEO TECHNOLOGY, vol. 14, no. 1, pp. 4–20, January 2004.

[3] K. Archana and A.Govardhan, "Enhance the security in the ATM system with multimodal biometrics and two-tier security," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, pp. 261–266, October 2013.

[4] U. Jayaraman, J. Viswanthan, A. K.Gupta, and P. Gupta, "Minutiae based geometric hashing for Fingerprint database," International Conference on Intelligent Computing, (ICIC -12), July 2012.

[5] A. Singh, S. Singh, and R. Kumar, "Secure swipe machine with help of biometric security," unpublished.

[6] A. T. Siddiqui, "Biometrics to control ATM scams: A study," International Conference on Circuit Power and Computing Technology ICCECT, pp. 1598–1602, 2014.