Transmission of Data Using Arm Based Privacy Protection QR-code

[1]prabakaran G, [2]bhakkiyalakshmi R
[1]Student, [2]Assistant Professor,
Embedded systems and Technology, SRM University, Chennai, India.
[1]gprabakaran333@gmail.com , [2]bhakkiyalakshmi.r@ktr.srm.ac.in

***Abstract*—The authentication system used in banks, to protect the assets of users is at high risk of safety. In order to overcome the safety issues, we proposed a system that allows the user to safely enter credentials and information to transfer money after launching LIVE-CD on stand alone in place and avoiding the possibility of entering credit card details (send or receive money without using of credit cards). The entered information is encrypted by common key crypto system and stored in a QR (quick response) code. The QR code encrypts our credit card details and also generates a One-Time Password (OTP). The arm processor will be checking the QR code details and perform two kinds of operation. It either carries out the transaction (if the entered password is correct) or stops the transaction (if entered password is wrong). In order to ensure safety in case if the QR code is used by unknown person it sends the information immediately to the particular account holder through e-mail (or) text message.**

IndexTerms*—Arm Processor, QR-code, Liquid crystal display, Webcam, LIVE -CD *(Keywords)

I. INTRODUCTION

The mainstay of this paper is a user safely enters credentials and information to transfer money without risk of peeping attack in Automated Teller Machine (ATM). ATM has some problems with authentication and transfer operation. First, as a problem with authentication, ATM uses ATM card and Personal Identification Number (PIN) principally. In other words, ATM is needed to type PIN using numeric keypad during authentication. Therefore, it is easy to assume that a password is stolen by peeping attack and secret filming during typing PIN. Next, as a problem with transfer operation, it is needed to take a long time during transferring money, because of many items which must be entered. As a result, ATM will be crowded.

As a solution of these problems, there is Internet bank that can transfer money on Internet. However, the Internet bank also has problems. Personal information is leaked by phishing sites and spyware such as key logger. Login sessions of Internet bank are stolen by Trojans. We proposed (figure1: illustrates the proposed system ATM hardware structure) the method of having three features [1]. First, it has resistance for a peeping attack. Second, it is hardly going to be crowded. Moreover, information is not stolen through a network. It makes bank transfer safety by using QR Code at ATM [2]. QR code is created for authentication at ATM by the method in advance after encrypting credential and operation information by common key crypto system and creating a Hash Code. The encrypted information is decoded by reading QR Code at ATM, creates a Hash Code in the server end and validates both the Hash Codes. Then, the system processes bank transfer in accordance with the decoded information.Finally, ATM displays confirmation screen for bank transfer including payees, branch, account and amount. By this unauthorized users are unable to find out the confidential information including the user's privacy.

II.SYSTEM ANALYSIS&RELATED WORK

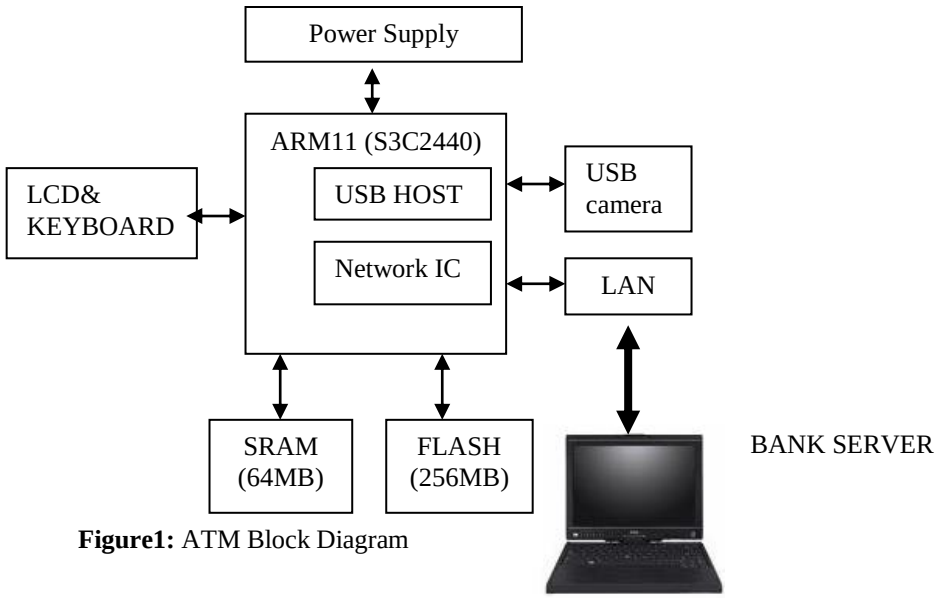

Figure1: ATM Block Diagram

In the conventional system, a QR-CODE is generated by the user to carry out the transaction. But the safety of the transaction is questionable. In order to ensure the safety of the transaction, we introduce the concept of creating a One Time Password (OTP), which will be created in advance and the user need to type the OTP to complete the transaction. If the user enters the wrong password in the ATM Centre, the Webcam installed with the system turns on automatically and captures the image of the user and sends it to the server. The following processes are carried out in our system.

- Initially we need to create a LIVE-CD, which is installedin Linux Ubuntu and Java Components.
- The application needed to create the QR-Code is embedded in the Live CD, where the user unpacks the jar file, executes the jar file, fills the money transaction information in the application. The application generates OTP and QR-Code for the given information.
- It creates an applet application and embeds our Webcam in it. The user shows the created QR-Code before the Webcam, for it to detect the hidden information in the QR-Code.
- If the User inputs wrong OTP for 3 or more times the Webcam snaps the user and sends it to the server.

III.CLIENT REGISTRATION, LIVE- CD GENERATION, QR CODE CREATION

A. Client registration

E-Banking Users have an initial level Registration Process at the web end. The users provide their own personal information for this process (figure 2: illustrates the Client registration details). The server in turn stores the information in its database and generates an application key, common key and a hash key for each and every user.

B.LIVE-CD generation and QR-CODE Creation

When the user registers an account at the bank, the bank creates a LIVE-CD that incorporates the application of creating QR-CODE. The bank issues a LIVE-CD containing an application for QR-Code Creation process for each and every authorized user [3]. The server also stores the key information in its back end. The server inserts the LIVE-CD into our PC and boots the system. Our Application boots from the operating system named Ubuntu.The user then unpacks jar file from the CD, extract it and run the QR-Code Creation Application. The user submits input to the application, and the application creates a HashCode named HashD, encrypts the whole information and creates a QR-CODE for the corresponding user. Basically the LIVE-CD modules consist of its two processes. First level process is performed by Bank side and second level process is done by customer side.

C.Bank Process

When the bank creates the LIVE-CD and also generates common key to encrypt information stored in QR-CODE [4]. The common key and hash key differ for each and every user.The bank keeps the common key and hash key with themselves for the authentication purpose. Using the Oracle database and apache Tomcat software, the bank will create relational data system for each and every user. The database consist of username, password, mobile no, e-mail id, common key, hash key, application key, user ID, account number, bank name, balance and branch code number.

D.User Process

After getting the LIVE-CD from the bank, the user boots the LIVE-CD each and every time for the transaction. Basically the LIVE-CD have Linux backend platform for its function and security purpose. When the user inserts the CD, it will be booted (like OS) and we need to enter the security password (LIVE-CD password) (figure: 3 and 4 shows the user process). Further the user enters the transaction details manually, like account holder name, bank name, branch name and amount. Finally the entered data are encrypted and the system will generate the QR-CODE and OTP.

IV.QR-CODE IDENTIFICATION AND TRANSACTION PROCESS

The user carries the QR-Code to the ATM and shows it in the display screen (figure 5:illustrates users created QR-CODE) The Scanner installed in the ATM System scans the QR-Code, identifies the information inside it and passes it to the Server. The Server decrypts the information and creates a HashD from the received information, and then compares both the HashD Codes (figure 6: shows the OTP matched screen at ATM machine). The server then authenticates the Common Key, Hash Key and the corresponding information and carries out the transaction process.

V. Illegal User Identification

Several Levels of Authentication will be done before forwarding the user to the Transaction Screen. The transaction process will be done and the money mentioned in the QR-Code will be transferred based on the processes. But if an illegal user tries to guess the One Time Password in the ATM Centre, our Webcams turns on automatically after 2 tries and snaps theuser 5 or more times and passes the illegal user's image to the server.

VI.EVALUATION RESULTS

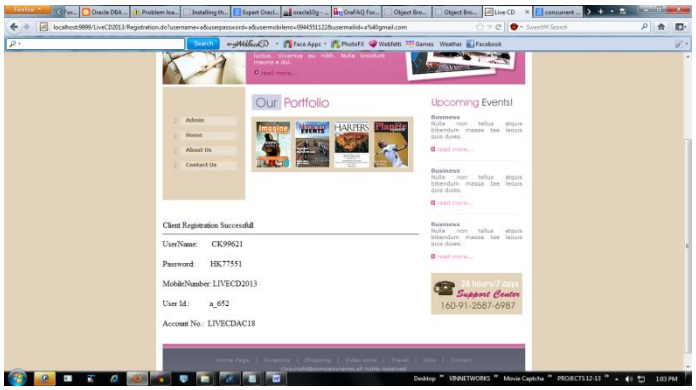

Figure 2: Client register

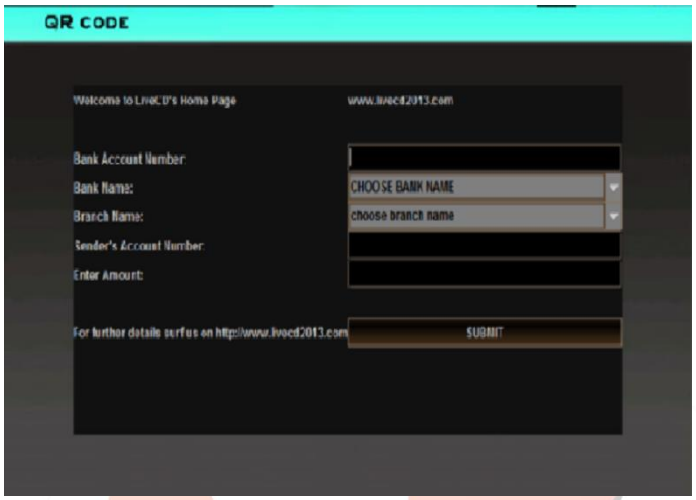

Figure3: Enter Account number&chose Branch location

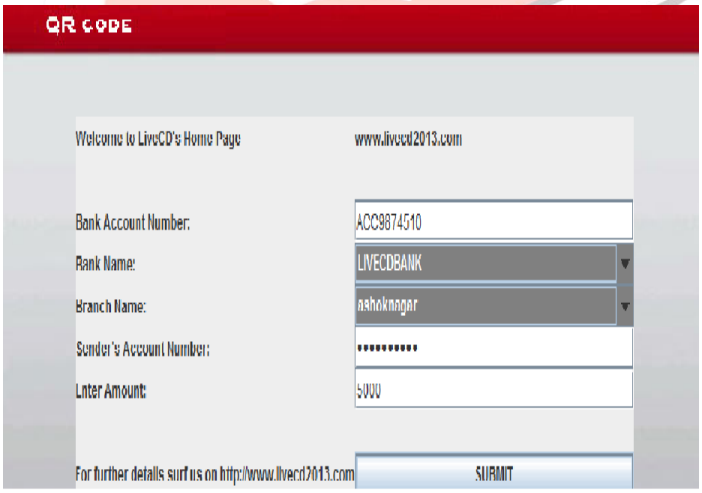

Figure4: Fill the all necessary options

Figure5: Generated QR-code

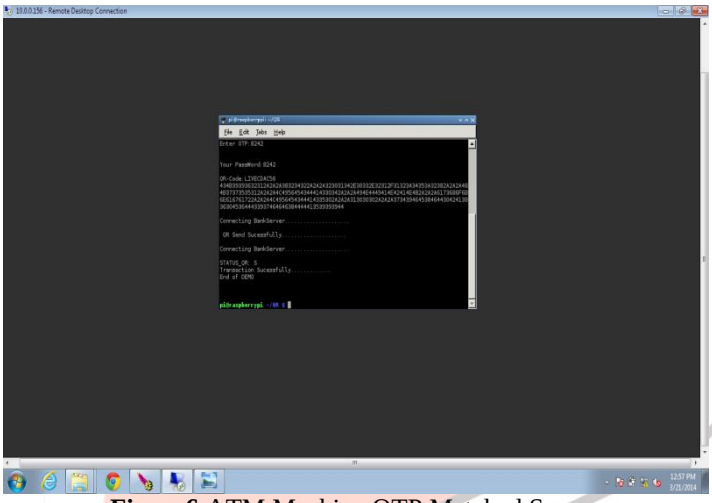

Figure6:ATM Machine OTP Matched Screen

VII.CONSULSION&FUTURE ENHANCEMENT

This paper presents an alternative method for authentication in ATM machine. Basically this method involves the transaction in an ATM by keeping the QR-CODE at the core part. Here we have made a progress in the user perspective of implementation of the technology. Use of credit and debit card can be completely replaced by using this technique.

The whole process is carried out by encrypting the data of credentials and generating the QR-code according to OTP, thereby ensuring the safety of the transaction. This project can be further improved by increasing its application areas by implementing it in all transactions, in addition to the ATMs.

REFERENCES

[1] ShoKurita, Kenji Komoriya, Ryuya Uda“Privacy protection on transfer system of Automated Teller Machine from Brute force attack”, 26th international Conference on Advanced information Networking and Applications, 2012.

[2] Sho Kurita, Shin Tezuka, Hirokazu Miyata, RyuyaUda, ”Proposal of Automated Teller Machine Transfer System with QR code”, IEICE, The 28th Symposium on Cryptography and Information Security (SCIS 2011), 2011.

[3] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino,” Impact of Artificial ”Gummy Fingers” on Fingerprint Systems,” Optical Security and Counterfeit Deterrence Techniques IV, Rudolf L. van Renesse, Editor, Proceedings of SPIE Vol.4677,pp.275-289,SPIE — The International Society for Optical Engineering,2002.

[4] Tsutomu MASTSUMOTO, Tomoki MORISHITA, LI Wen,”Liveness Detection and Failure to Enroll in Biometrics (3)-A Research on Vein Pattern Based Authentication, Part2-”, IEICE, ISEC2006-8, pp. 53-60, 2006/5 (Japanese).