SAFA

(Secure Authentication For ATM)

Er.Sijo Cherian
Assistant Professor, Department of Computer Science and Engineering
Saintgits College of Engineering,Kottayam
Kottayam, India

Divya Siby
Btech Students, Department of Computer Science and Engineering
Saintgits College of Engineering,Kottayam
Kottayam, India

Neelima N
Btech Students, Department of Computer Science and Engineering
Saintgits College of Engineering,Kottayam
Kottayam, India

Neethu K Philips
Btech Students, Department of Computer Science and Engineering
Saintgits College of Engineering,Kottayam
Kottayam, India

Preethi Krishna K
Btech Students, Department of Computer Science and Engineering
Saintgits College of Engineering,Kottayam
Kottayam, India

I.J.I.R.C.T

***Abstract*—SAFA is a secure authentication system developed for ATM. It is a solution to the endless types of frauds. The illegal activities of fraud obtain credit card information using latest technologies. This user friendly system is controlled by an admin and utilized by a user. The user can use this model to login to the system with the help of SAFA application, which gives secure authentication and protects the data in our system from attackers. In the case of loss of phone, there is a provision to block the use either by the admin or by the user. There is a web portal through which both the admin and the user can manage their functionalities.**

***Keywords*— SAFA, Authentication**

I. Introduction

Our aim is to provide an authentication for ATM via a secure pin. The increasing number of shoulder surfing attacks and replay attacks [3] [4] [5], demand a more secure authentication system. In the present era of smart phone applications, this one-time-pin generated provides more security. The hidden four digit pin will be sent to the smartphone application. There is no need to carry the credit card. SAFA application finds a place due to its user friendly nature. Also the pin generation requires the username and password from the user apart from the details of transaction, which adds to the security.

II. Methods

A. Secure authentication via SAFA app

There is absolutely no need to carry the ATM card for authentication. Once connected to the network, the user can scan the QR code generated on the ATM terminal. Then the user needs to provide username and password. Based on the entered data and information from the QR code, the verification is done and subsequently a pin will be generated and sent to the ATM. Only 4 digits will be visible on the terminal. The hidden digits are sent to the application. On entering these hidden digits, the required authentication takes place.

B. One time pin generated on each access

The one time pin is generated as soon as the verification of user and ATM details takes place. Since there is a different pin generated on each access, the shoulder surfing attacks will be in vain. Also the user need not remember the pin for authentication as it changes each time. In order to receive this pin, user must enter the username and password. So even if the phone is lost, the attacks will be unsuccessful.

C. User friendly approach

SAFA system is user friendly as the user need not carry ATM card for transactions. The user can easily register to the SAFA application via the bank website by providing the email id. ATM information i.e. amid and time is retrieved by server by scanning the QR code. The user just need to provide username and password. The pin generation takes place within seconds. Also the user has an option to change the device through the bank website as the application of a particular user can work only in one device at a time. Even if the phone is lost, the user can easily block the device through the bank website. In case the password is forgotten, user can get a new password by just entering him email id. New password will be sent to the user's email.

III. System Model

We define the SAFA system model [1], which will allow ATM users to perform secure authentication at ATM terminals. SAFA depends on three parties: the ATM terminal, the user, and the bank server. We have defined the system currently for a single system. This can be extended in future.

1) Server: The SAFA server is owned by the bank and stores the user's profiles as well as ATM information. The server communicate with the user application and the ATM terminal. In our simulations, we have ensured proper wifi connection in the surroundings.

2) ATM Terminal: Each ATM has a unique location identifier, which is assigned by the bank. The ATM surroundings have a proper network connectivity and can communicate with the bank through a secure connection.

3) User: The user gets a valid pin for authentication at the access terminal. The user should have a personal smart phone for using the SAFA service for secure authentication of ATM service access. The user can also choose to use a wearable smart device for using the SAFA service. However, the relatively larger impersonal display of the mobile device, compared to the wearable smart device, creates some vulnerability for attacks by observation. The SAFA application is installed on the wearable device or the smart phone.Initially the application need to be configured in the device.This requires a username and password.Once the user details are verified,they need not configure it again.The password is automatically generated at the bank server and sent to the email of user on registering with the SAFA application The SAFA service on the cloud allows the user to store and save the SAFA information of the user,which is used in the SAFA protocol. If the user forgets the password,a new password will be sent to the user on specifying the email id.

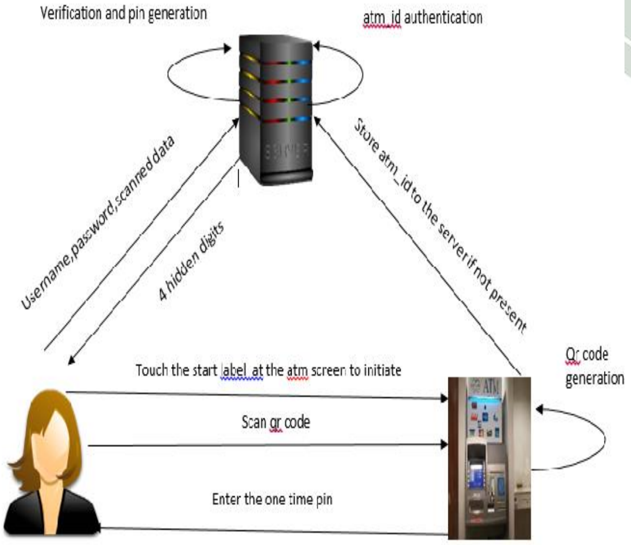

Verification and pin generation
atm_id authentication
Username,password,scanned data
4 hidden digits
Store atm_id to the server if not present
Qr code generation
Touch the start label at the atm screen to initiate
Scan qr code
Enter the one time pin

Fig. 1. SAFA architecture.

Our protocol [2] has various interactions between the three parts of the SAFA system: The user and the ATM terminal, the terminal and the bank, and user and the bank. The sequence of interactions and message transfer in the protocol is described as follows.

Step 1: [Registration] The user must register with SAFA application through the bank website.

Step 2: [Password generation] A system generated password will be sent to the user's email id.

Step 3: [Configuration] After installing the application in the smart phone,configure it using the email id(username) and password.

Step 4: [Initial Trigger] For doing transaction the ATM terminal will display a "Start" prompt on the ATM screen and the user touches the screen to begin the transaction.

Step 5: [ATM authentication] If the atm_id is not already present in the database,it will be added to the database and we must initiate it by touching the start button.If present,the atm is authenticated.

Step 6: [QR code generation] A new transaction begins and we will be shown a QR code which consist of information like atmid, current date and time.

Step 7: [Scanning QR code] The QR code should be scanned using the scanner in the smartphone and the information contained is verified with that in the bank. In case there is no QR code scanner in the smartphone, there is a link in the application where the user can download the scanner from.

Step 8: [Verification] after the scanning phase, a 4-level checking is done i.e., if the username and password entered are correct or not, if the atmid is valid or not (one that is present in the database), if the app-status is blocked/unblocked and if the transaction status is null or not. At the beginning of the transaction, the transaction status is set active. At any time during authentication, if cancel button or exit button is pressed, the transaction status will be set to null.

Step 9: [One Time Pin Generation] On successful scanning and authentication of the details scanned, the server generates the pin.

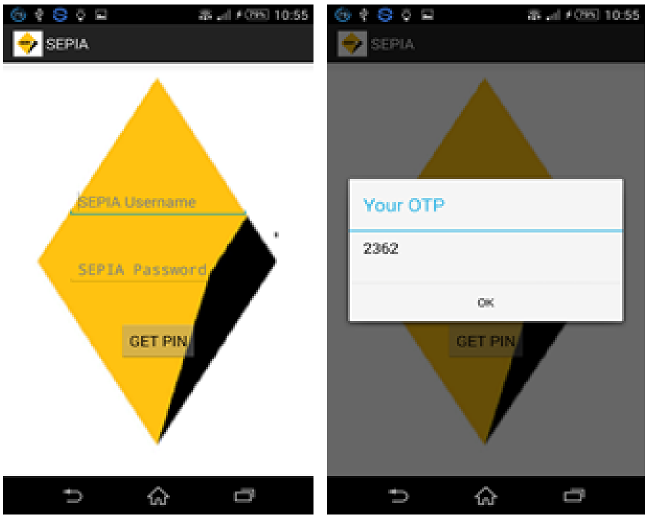
Step 10:[Server response] The four digits of the pin generated will be sent to the SAFA application.

Step 11: [User response] The last 4 digits of the pin, displayed in the application will be entered to the last 4 invisible characters of the 8 digit pin template displayed on the ATM screen by the user.

Step 12: [Secure authentication] After checking, if the user authentication is successful, the user will be redirected to the transaction page else the transaction will get cancelled and the ATM will be back to start terminal.

IV. Usability Study And Analysis

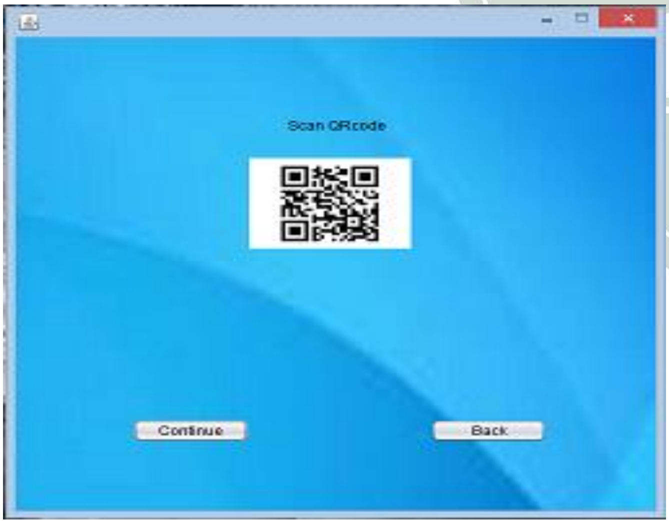
The usability study was conducted in two stages. In stage 1,both server and atm were simulated using a single PC and application was run on a smartphone. A study was done on the basis of 10 different users. QR code scanning was done for 10 times. The mean response time was found to be 1 second. The error rate for 4 level checking during these times was 20%.Once verification was done, one time pin generation was quick.4 hidden digits were sent immediately to the SAFA app with an average of 2 seconds.



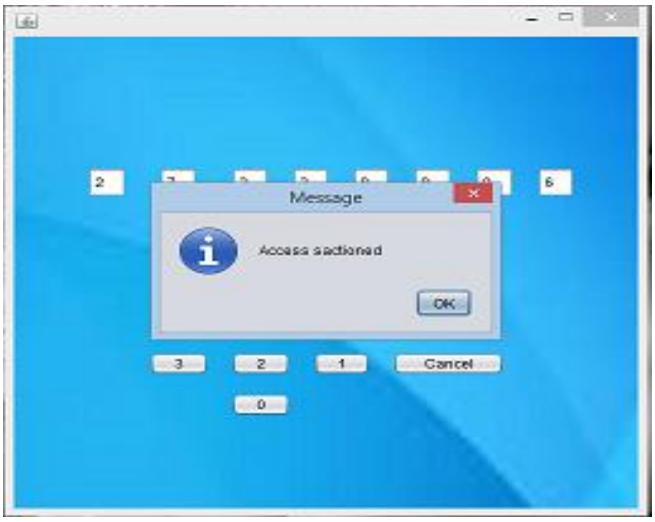
2(a) 2(b)

Fig. 2. (a) User verification (b) Getting pin.

10 participants entered the 4 digits to the atm terminal and mean time taken by all of them for successful attempts was 1500.7 milliseconds. In stage 2, server and atm were simulated on different PCs. There was connection delays in this case. But the response time for the whole system was reduced only by 2%.



3(a)



Access sactioned

3(b)

Fig. 3. (a) Generated QR code (b)Sanctioned access.

Conclusion

This paper helps to ensure security in atm transactions from the rising number of frauds. The 4 level verification system improves the security. One account can have the application configured to one and only one phone at a time i.e getting the application by an intruder is worthless. Also the SAFA system can be easily blocked by the user on loss of phone. In total, the system is simple, cost-effective and efficient

Currently SAFA system is simulated for a single bank which can be extended further. Also SAFA can be a solution for any system which involves secure authentication such as door locking system since SAFA is simple and user friendly.

References

[1] [1] Rasib Khan, Ragib Hasan, and Jinfang Xu SECRETLab, Department of Computer and Information Sciences University of Alabama at Birmingham, Birmingham, AL 35294, US ," SEPIA: Secure-PIN-Authentication-as-a-Service for ATM using Mobile and Wearable Devices"at,2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering .I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[2] M.Priyadharshini1, G.Manisha,Assistant Professor, Dept. of CSE, Valliammai Engineering College, Chennai, Tamil Nadu, India," Quick Response code for ATM transaction Using Face Recognition",in International Journal of Innovative Research in Computer and Communication Engineering Vol.3 special issue 8,October 2015.

[3] Minu C.M,Sheema Madhusudhanan,Prof.P.Jayakumar, MachinesDept. of CSE (Cyber Security) Sree Narayana Gurukulam College of Engineering ,Kadayiruppu, Kerala, India ,"A Study On Vulnarabilities of Automatic Teller Machine" at International Conference on Emerging Trends in Engineering & Management 2016 in IOSR Journal of Computer Engineering.

[4] S. Raj and A. Portia, "Analysis on credit card fraud detection methods," in Computer, Communication and Electrical Technology (ICCCET), 2011 International Conference on, March 2011, pp. 152–156.

[5] N. Sethi and A. Gera, "A revived survey of various credit card fraud detection techniques," International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, pp. 780 – 791, April 2014.

I.J.I.R.C.T