Implementation of Mobile Banking Authentication System Using RC5 Encryption Algorithm

Moe Pwint Phyu, Dr. Win Win Thant

University of Computer Studies, Yangon (UCSY)

mmpwint7@gmail.com,winwinthant@gmail.com

ABSTRACT

Nowadays, Mobile Banking (MB) System is performing of finance related functions on a mobile device. MB can be used anywhere you take your device and fast banking today. Current MB confidentiality and authentication are challenging and then identified as major security risks. In this paper, MB system is implemented on confidentiality, authentication and verification of security channels to protect the system's security risks. To protect the confidentiality and authentication, RC5 encryption algorithm is used to encrypt PIN (Personal Identification Number) number in MB system. Then, CAPTCHA image grid view is used to protect the verification. Therefore, this system can fulfill not only the requirement of the security of mobile user but also the security of banking database system.

Keywords: Mobile Banking System, Rivest Cipher 5(RC5), CAPTCHA Image

1. INTRODUCTION

Mobile banking is a revolution that is driven by the world's one of the fastest growing sectors mobile communication technology. Data at the user end with mobile device is not only sensitive but also the data of database at the MB server end is sensitive. A very key component of protecting information confidentiality would be encryption. Encryption ensures that only the right people can read the information. Encryption is very widespread in today's MB system and can be found in almost every major protocol in use. Therefore, in this paper, secure MB authentication system has been configured by using RC5 encryption algorithm and CAPTCHA images grid view. Firstly, PIN number of mobile user is encrypted by using RC5 encryption algorithm for authentication and confidentiality security goals in system. Secondly, CAPTCHA image is used for extra security or verification in system. Encryption of PIN number and CAPTCHA image are used for identified the uniqueness of authorized person. There will mainly protect that risk of unauthorized persons using the mobile phone for MB. The MB application is very useful for more secure the user end and bank end. It can also save the time of mobile users. Moreover, mobile users can safely access that their banking activities from anywhere. Due to the obvious security advantages of mobile banking application, now the system has gained great popularity in more places.

The rest of the paper is organized as follows. Related works of the system are described in section 2. Section 3 explains the background theory. The design and implementation of the proposed system are presented in section 4. Section 5 contains scope and limitation of the system and section 6 describes conclusion of the system. Finally, section 7 presents future work to further improve our MB system.

2. RELATED WORK

There have been numerous studies that associated with banking system and the use of

different encryption algorithms from other thesis papers. This section describes related works associated with the system.

The authors of [1] described secure SMS banking delivery. SMS encryption is used in every banking transaction of system. But, SMS centre server can easily view sensitive details since the message is in plaintext.

The authors of [2] presented mobile banking SMS security using combine cryptographic algorithms called Diffie Hellman key Exchange, AES and SHA-256 hash. Diffie Hellman key Exchange Algorithm for exchanging key, AES for encryption/decryption and SHA-256 for generating hash value are used. Their system is used to provide a peer-to-peer SMS security that guarantees the confidentiality, authentication, integrity and non-repudiation security services.

In 2010, the authors [8] described a new user authentication scheme for mobile banking systems. They reported the security weakness in the authentication scheme used by EKO and then proposed scheme which relies on the user of PIN and printed codebooks. According to their research, their new scheme provides better protection to PIN as they are transmitted over the network.

The authors [9] presented FPGA based Sliding Window Architecture with RC5 Encryption. Their purpose was to reduce the waiting time by using sliding window method. The sliding window is a popular data link layer protocol and it is widely used in data transmission methods. RC5 is also used to encrypt the data while data transmission in their thesis. The future scope of their work will be where priority of the data has a given more securely emphasis with sliding window.

3. BACKGROUND THEORY

This section describes the mobile banking technologies, background theory of RC5 encryption algorithm and the use of CAPTCHA image in MB system.

3.1 Mobile Banking Technologies

Mobile Banking Technologies [2] can be categorized into two environments: **Server-Side Technology** and **Client-Side Technology.**

***Server-Side Technology*:** It is built on a server, away from the user's mobile device. Example of server-side technologies would be SMS(Short Messaging Service), IVR(Interactive Voice Response), USSD(Unstructured Supplementary Service Data) and WAP(Wireless Application Protocol).

Client-Side Technology: It is built on the user's mobile device. Example of client-side technologies is J2ME (Java 2 Micro Edition).

In server-side applications, the user data that enables the processing of transactions, such as account/history details, are typically stored on a server at a bank.

In client-side applications, the user data is typically stored on the application, or entered by the user, and encrypted by the application in the mobile device.

3.2 RC5 Encryption Algorithm

Rivest Cipher 5 (RC5) is a symmetric encryption algorithm developed by Roland Rivest, it was designed to have the following objectives:

Symmetric block cipher: The same secret cryptographic key is used for encryption and for decryption. The plaintext and cipher text are fixed-length bit sequences.

Fast: RC5 is a simple algorithm and is word oriented. The basic operations work on full words of data at a time.

Variable number of rounds: The number of rounds is a second parameter of RC5. This parameter allows a tradeoff between higher speed and higher security.

***Variable*-length cryptographic key:** It is the third parameter of RC5. Again, this allows a tradeoff between speed and security.

Simple: RC's simple structure is easy to implement and eases the task of determining the strength of the algorithm.

Low memory requirement: This property makes the algorithm suitable for smart cards and other devices with restricted memory.

High security: It should provide high security when suitable parameter values are chosen.

***Data-dependent rotations*:** RC5 incorporates rotations (circular bit shifts) whose amount is data dependent. This indicates to strength the algorithm against cryptanalysis [4].

3.2.1 Description and Features of RC5

RC5 is a parameterized algorithm, and a particular RC5 is designed as RC5-w/r/b [6]. Table 1 summarized these three parameters.

Table 1. Parameters of RC5

Para meter	Definition	Allowable Values
w	Word size in bit, RC5 encrypts 2-word blocks	16,32,64,128
r	Number of rounds	0, 1, …, 255
b	Number of 8-bit bytes in secrete key K	0, 1, …, 255

RC5 encryption algorithm consists of three main components. There are: key expansion, encryption and decryption.

3.2.2 Key Expansion

The key-expansion algorithm expands the user's key K to fill the expanded key table S, so that S resembles an array of t = 2 (r + 1) random binary words determined by K [7]. Figure 1 illustrates the technique used to generate the subkeys.

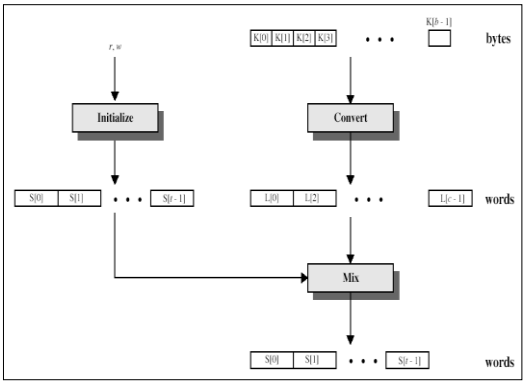

Figure 1. Key Encryption of RC5

3.2.3 Encryption and Decryption of RC5 Algorithm

***Encryption Algorithm*:**

The two w-bit words inputs are denoted as register A and register B.

```
A = A + S [0];
B = B + S [1];
for i = 1 to r do
A = (( A ⊕ B ) <<< B ) + S [ 2 * i ];
B = (( B ⊕ A) <<< A ) + S [ 2 * i + 1];
```

***Decryption Algorithm*:**

The two w-bit word inputs are denoted as register A and register B.

```
for i = r downto 1 do
B = ((B – S [2 * i + 1]) >>> A) ⊕ A;
A = ((A – S [ 2 * i ] >>> B) ⊕ B;
B = B – S [1];
A = A – S [0];
```

The outputs are in register A and register B.

3.3 The Use of CAPTCHA Image

The completely mean of CAPTCHA is "Completely Automated Public Turing test to tell Computers and Humans Apart" [5]. In simple words, CAPTCHA is the word verification test. Mostly, CAPTCHA words as images are used in web-based email services like Gmail, Yahoo, etc. CAPTCHA images are difficult to remember because there are shown as distorted words in images. There are useful for high level of secure MB system. Therefore, CAPTCHA images will add as extra security feature to satisfy verification. In this system, CAPTCHA images grid view is used as verification process for more secure MB system in this system.

4. DESIGN & IMPLEMENTATION OF THE SYSTEM

This system is implemented in Android and Java programming language, and mysql database. Socket server is used in java programming to connect android application. And, same Wi-Fi internet connection must need for data transmission between socket server and MB android application.

In this section, proposed system architecture, proposed mobile banking services, system design diagrams and implementation of mobile banking authentication and confidentiality are included.

4.1 Architecture of Mobile Banking System

The main components of the architecture of the MB system are mobile device which already install mobile banking application, same Wi-Fi connection between mobile device and bank, and running banking server.

The architecture of the proposed system is shown in figure 2.

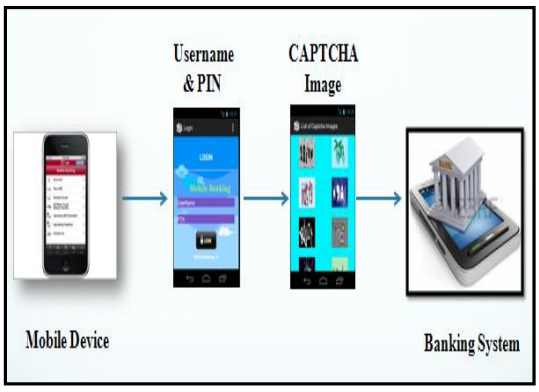

Figure 2. Mobile Banking System Architecture

As shown in figure 2, if mobile user has already open MB account, user can easily login into the system. User enters username and PIN number receiving from email while MB account sign up. If first login step is successful, user will need to choose correct CAPTCHA image from random images gird view. If this step is also successful, user can perform MB transactions securely.

4.2 Services of Proposed System

The general services of proposed system can be considered as follows:

***Mobile account transfer*:** MB account transfer service make internal funds transfers between Accounts.

***Check Current Balance*:** MB users can view their current balance as easily.

***Show History*:** MB users can view their transaction information associated with transfer, deposit and withdrawal as clearly.

***Deposit*:** MB users can perform deposit function in their account itself.

***Withdrawal*:** MB users can perform withdrawal function in their account itself.

***Change PIN*:** MB users can change PIN number with their desired PIN number.

4.3 Process Flow of Proposed System

The general process flow of proposed MB system is described in Figure 3.

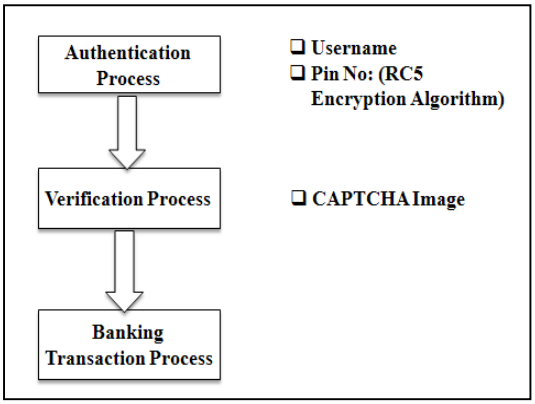

Figure 3. Process Flow of Proposed System

In authentication process, username and PIN number are encrypted by using RC5 algorithm. In verification process, CAPTCHA images are shown randomly in grid view for more secure level of system. After both authentication process and verification process are completely performed, mobile users can easily and faithfully access their banking transaction processes.

4.4 System Flow of Proposed System

The system flow diagram and its explanation are described in Figure 4.

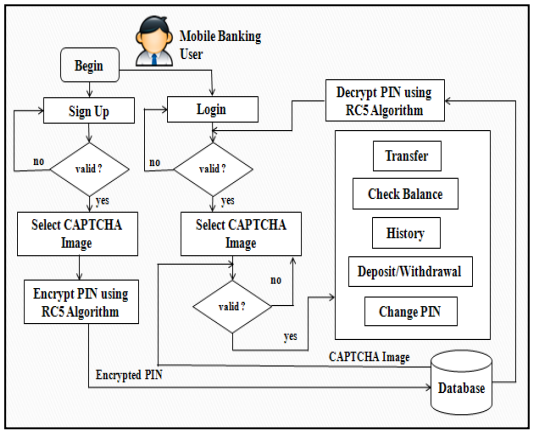

Figure 4. System Flow of Proposed System

User can also easily create new MB account from device that installing mobile banking application. If mobile user can login successfully, user can transfer mobile money from one account to another account, check current balance, view transaction history and can easily change PIN as like password.

4.5 Mobile Banking Application

At client side or mobile user side, MB application will need to install in user's mobile phone. After installation, user can use easily by clicking "Start" button. User will see welcome mobile banking page. User can choices create account, login, about and help functions from this page. About and help functions are just information pages.

4.6 Identity Authentication of User Sign Up

Create account button must click if mobile user is new user for MB system. At this stage, user will fill required information to create new account. After filling information, user will choose only one CAPTCHA image from sequential CAPTCHA images grid view and must need to remember that this chose the CAPTCHA image. After this step also finished, user will receive confirmation mail which includes login username, account number and PIN number. Email confirmation will satisfy the authentication security because authorized person only can accept the information through email.

4.7 User Data Confidentiality

In MB server-side, user's entered username is generated as login username which first and last characters of username are combined and then this combination is more added with random 6 digits. And then, user entered PIN number (6 digits) is encrypted with RC5 encryption algorithm. Encrypted data is stored in banking database for confidentiality of security.

4.8 Mobile Banking User Login

In client-side, user can login by using login username and PIN number from confirmation

mail. If username and PIN number are valid, user will correctly select CAPTCHA image from random images grid view as a next step. User can use banking transaction services if CAPTCHA image selection is also valid. If not valid, user must again login from first step with login username and PIN.

5. SCOPE & LIMITATION

Mobile banking system is designed for android phone. Essentially need to install this MB application in your android phone. User interface is only in English. User can login only with his login username, PIN and CAPTCHA image. In this system, deposit, withdrawal and transfer functions associated with finances are available. And then, RC5 algorithm implemented 32 bits two inputs plaintext, 12 rounds and 32 bit secret key while encryption.

6. CONCLUSION

This thesis paper presents that mobile banking is as safe as it implements the RC5 encryption algorithm and CAPTCHA image as security measures. RC5 provides a satisfactory balance between power consumption, security strength and computational time. From mobile banking database's point of view, this system will more provide the confidentiality of security channel by using the RC5 encryption algorithm and then this system will also improve the authentication from mobile banking user's point of view because of this system contains the email sending function. Moreover, selection of CAPTCHA image from random images gird view will improve the verification process. Thus, this system can create better secure of MB system with users are satisfied.

7. FUTUTE WORK

This paper proposes to implement the secure mobile banking system. In future, more secure, power saving and fast encryption algorithms will use instead of RC5 encryption algorithm in mobile banking system. Furthermore, biometric methods such as fingerprint recognition, face recognition etc. can be used to support more system security. This paper's evaluation uses only deposit, withdrawal and transfer functions. In future, calculations of interest rating can be added within system like real bank. And, MB applications will design not only android devices but also iOS devices for all users in future.

References

[1] Abunyang, E.(2007), Secure Framework for Delivery of SMS-banking Services, Student Number: s0535249, Radboud University Nijmegen, Netherlands.

[2] Gavin Troy Krugel, info@troytyla.com, 2007, **"**Mobile Banking Techology Options", Finmark Trust, India University.

[3] Masaya Y., and K. Sakaun, 2011. "Dedicated hardware for RC5 cryptography and its Implementation".

[4] Mowafak Hasan and Hasan Al-Shalabi, 2005. "Modified Cryptanalysis of RC5", Collage of Computer Engineering and Information Technology, Al Hussein Bin Talal University, Jorddan.

[5] Mrs. A.Angel Freeda (Asst. professor), M.Sindhuja and K.Sujitha (Students), April-May, 2013, "Image CAPTCHA Based Authentication Using Visual Cryptography".

[6] Rivest, R. L. (1994). "The RC5 Encryption Algorithm" (Proceedings of the Second International Workshop on Fast Software Encryption (FSE) 1994.

[7] Rivest R. L., "The RC5 Encryption Algorithm," Dr. Dobb's Journal, no. 226, pp. 146-148, January 1995.

[8] Saurabh Panjwani, Edward CutrellMicrosoft Research India {saurap, cutrell}@microsoft.com.

[9] Vishal Parkar, Computer, Rajendra Mane College of Engineering &Technology, Ambav, India.