A Practical Approach for Secure Internet Banking based on Cryptography

Syeda Farha Shazmeen[1], Shyam Prasad[2]

[1]Department of Information Technology, Balaji Institute of Technology and Science, Warangal, A.P, India, 506331
farhashazmeen@gmail.com
[2]Department of Information Technology, Balaji Institute of Technology and Science, Warangal, A.P, India, 506331
shyambitswgl@gmail.com

Abstract: There are a continuously growing number of customers who use Internet banking because of its convenience. But the security and privacy of Information may be one of the biggest concerns to the Online Banking users. The problem with Online banking applications is that they send data directly to customer in plain text form compromising with security. The solutions to the security issues require the use of software-based solutions that involve the use of encryption algorithms. For this we propose a challenge/response -based short-time password authentication methods using Symmetric cryptography in combination with Software Security model. In this approach bank hides customer transaction data is secure SMS using IDEA symmetric cryptographic algorithm and send it to customer application supported handset. Customer application decrypts data in secure manner the encryption and decryption are characterized by a secret key that the legal parties have to posses. So, in face of the current security issues and the growing number of attacks and consequent frauds, new internet banking systems should be designed as to provide better authentication and identification methods. And these methods can be implemented to the Mobile banking to address the Security concern.

Index Terms: Internet Banking, security standards, short-time passwords

I. INTRODUCTION

The security models for online banking systems currently in use are strongly based on Internet banking user identification and authentication methods[2], which are also the components where most Internet banking systems' vulnerabilities are found. The existing SMS system does not have any built-in procedure to authenticate [1] the text and offer security for the text transmitted as data, because most of the applications for mobile devices are designed and developed without taking security into consideration.

1(a) Security

Security of the transactions is the primary concern of the Internet-based industries. The lack of
Security may result in serious damages the security issue [3] will be further discussed in the next section along with the possible attacks due to the insufficient protections. The examples of potential hazards of the electronic banking system are transferring funds, and minting electric currency, etc.

1(b) Authentication

Encryption may help make the transactions more secure. The Internet of today has become an integral part of our
Everyday life and the proportion of users expecting to be able to manage their bank accounts anywhere anytime is constantly growing [4]. As such, Internet banking has come to age as a crucial component of any financial institution's multi-channel strategy. Based on the assumption that only an authentic user is able to do so, successful authentication eventually enables an authorized user to access his private information.[5]

1(c) Short-Time Password Solution

Considering today's pervasiveness of malicious software and phishing attacks, any Internet banking solution must be resistant against stealing attacks. For this we propose a challenge/response-based short-time password authentication method using symmetric cryptography in combination with a Software Security Model [6, 7]. The short-time password solution is in use at in software-based security systems, the coding and decoding of information is done using specialized security software.

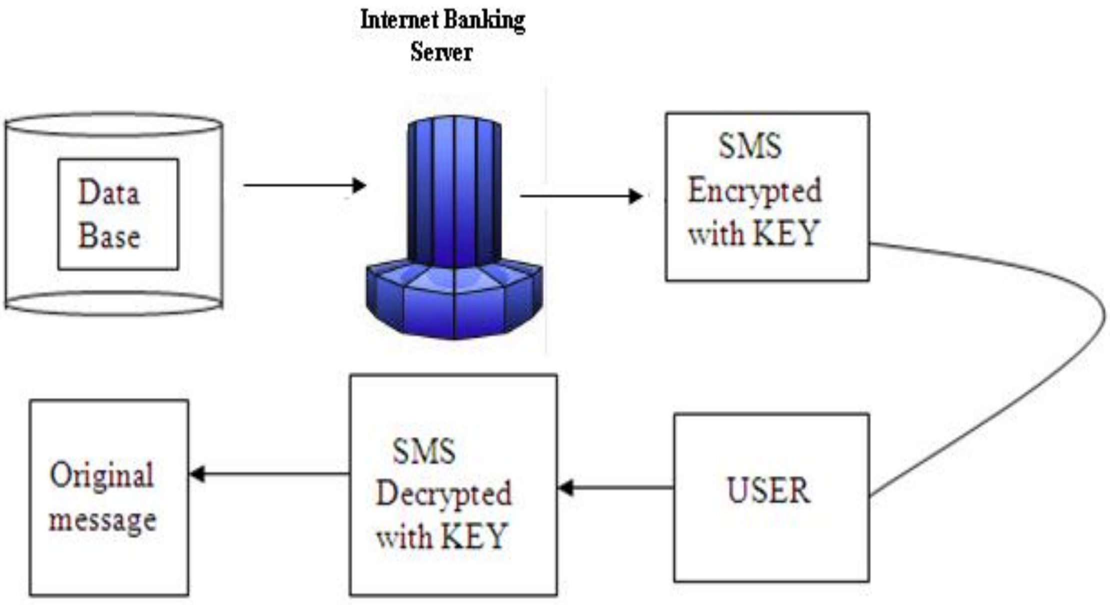


Fig 1: Architecture of Secure Transaction

The Fig (1) shows the Architecture of the Secure Transaction, where the Bank Server sends the Encrypted message to the User and the User Decrypt's the message [8, 9], the encryption and decryption are characterized by a secret key that all legal parties have to posses. The application is develop using programming language Java and the J2ME environment. [10, 11]

II. Secure SMS Messages Using Cryptography

Most of the attacks directed at online banking systems target the user (the weakest link in the Chain), focusing on obtaining authentication and identification information through the use of Social engineering and compromising the user's Internet banking access device in order to install malware which automatically performs banking transactions [13,14], apart from obtaining authentication data. This fact indicates that secure internet banking systems should provide security mechanisms as user independent as possible, mitigating the risk of user related information's leaks and security issues affecting the system and leading to fraud [15].

2(a) SMS Security Algorithm: The International Data Encryption Algorithm (IDEA)

SMS messages are sometimes used for the interchange of confidential data such as social security number, bank account number, password etc [23]. A typing error in selecting a number when sending such a message can have severe consequences if the message is readable to any unauthorized receiver. In this application for sending encrypted SMS messages using cryptographic methods based on the IDEA Algorithm. The encryption algorithm is characterized by a secret key. The application is develop using programming language Java and the J2ME environment [12].

International Data Encryption Algorithm (IDEA) is very secure; IDEA operates on 64 bit blocks using a 128-bit key, and consists of a series of eight identical transformations (a *round*) and an output transformation (the *half-round*). The processes for encryption and decryption are similar [16, 17]. IDEA derives much of its security by interleaving operations from different groups — modular addition and multiplication, and bitwise eXclusive OR (XOR)

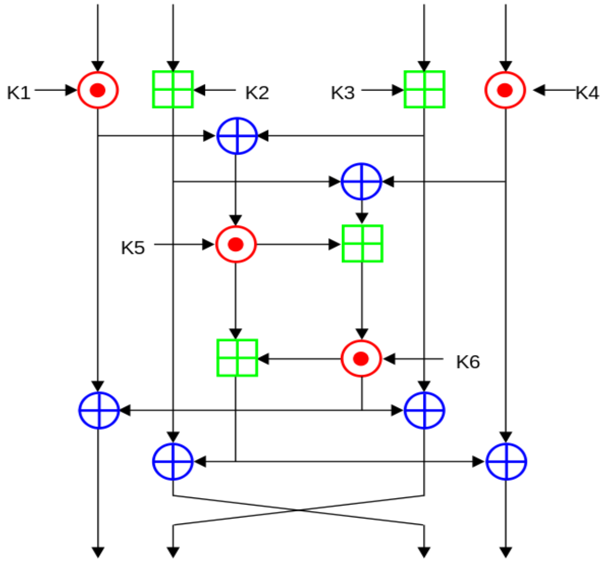


Fig 2: An encryption Process of IDEA

III. Implementation

In addition, communicating over wireless networks with a mobile device brings its own set of inherent risks. With knowledge and equipment, it is possible to intercept data most anywhere between your device and the end point of your intended communication [18, 19]. A J2ME system which is installed in all the mobiles of the users those who are registered with this system. The user who received the encrypted message has to enter into this application and provide the corresponding key to decrypt and see the message. The encryption application-related data is in Java 2 Micro Edition (J2ME) application (MIDlet).

3(a) Bouncy Castle

Bouncy Castle is an open source encryption library; there is a lightweight version suitable for use with J2ME. Bouncy Castle is an open source Java API for encrypting and decrypting data. Bouncy Castle [21] is a Java Cryptography Extension (JCE) provider. JCE is an optional package that provides support for ciphers, keys, and message authentication within the Java 2 Platform, Standard Edition (J2SE). Essentially, a provider offers one or more algorithms for the encrypting and decrypting of data. To date, Bouncy Castle supports over 20 engines. **ProGuard** [22] is an open source Java class files obfuscator. This is used to obfuscate the contents, which requires less memory to store.

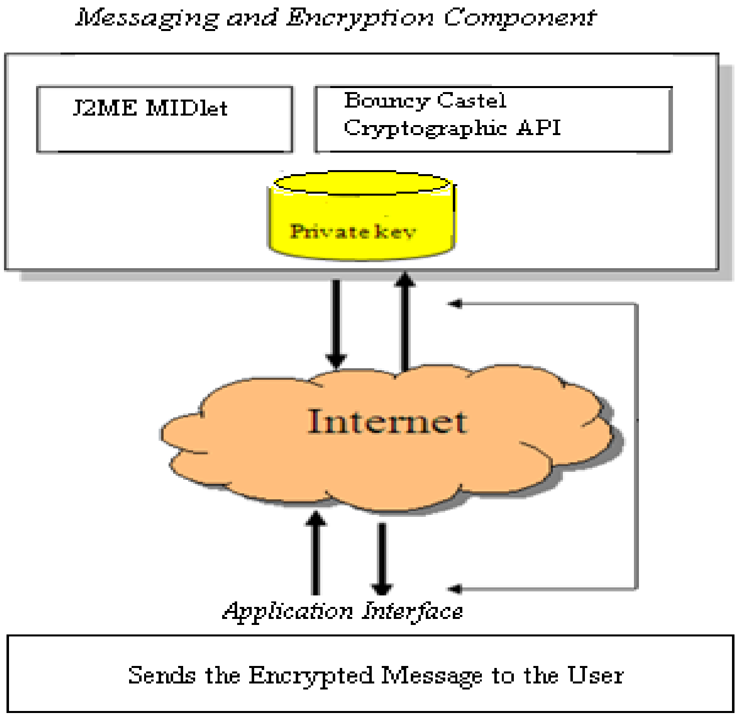


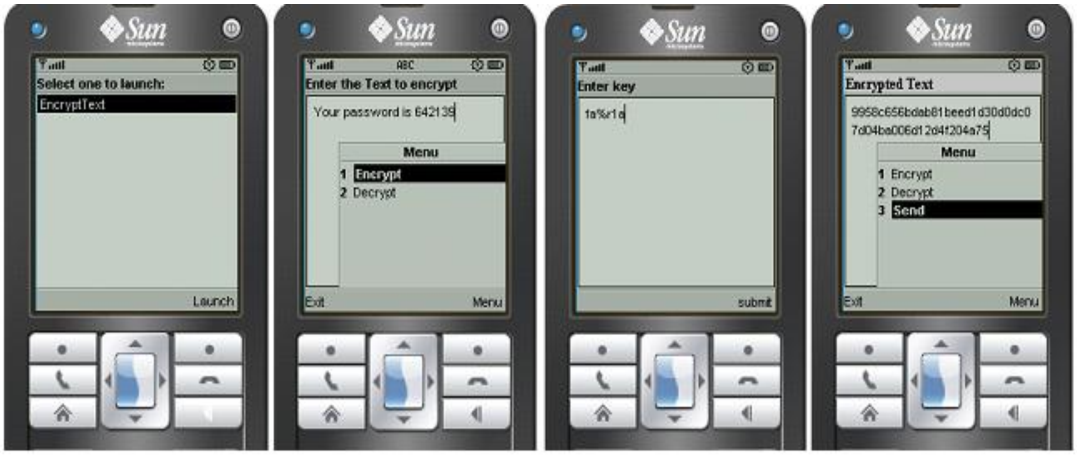
Fig 3: Shows the Messaging and Encryption Component

To implement the following process, the Sun Microsystems Wireless Toolkit formerly known as Java 2 Platform, Micro Edition (J2ME) Wireless Toolkit) is used. It is a state-of-the-art toolbox for developing wireless applications that are based on J2ME's Connected Limited Device Configuration (CLDC) and Mobile Information Device Profile (MIDP), and designed to run on cell phones, mainstream personal digital assistants, and other small mobile devices. The toolkit includes the emulation environments, performance optimization and tuning features. Wireless Toolkit is an integrated development environment (IDE) creates J2ME MIDlet [20]. The WTK contains an IDE, as well as the libraries required for creating MIDlets.

A MIDlet is created which accepts the text to be encrypted along with the key (Secret key) by using which the Encryption process is done by using IDEA algorithm. The Symmetric ciphers use the same key to encrypt and decrypt data, which is known as *secret key*. That is, the value of the key is kept secret between the two parties -- those who encrypt the data and those who decrypt it.

The J2ME MIDlet which accepts the text and encrypts the text which is send to the user, when the user receives the Encrypted text can decrypts the text to find the original text. The Short time passwords or any Bank related confidential data can be secured by the using the Cryptographic techniques.

The Following screens demonstrate the Experimental Analysis.



Select one to launch:

EncryptText

Enter the Text to encrypt

Your password is 642139

Enter key

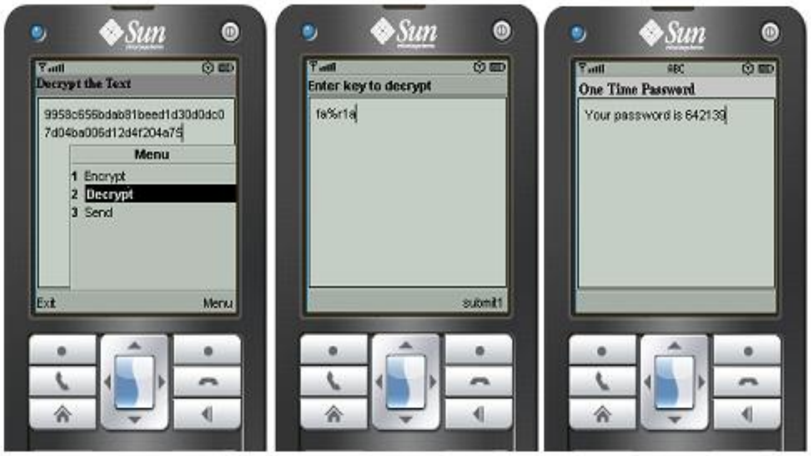
1a%r1a

Encrypted Text

9958c656bdab81beed1d30d0dc0
7d04ba006d12d4f204a75

Fig (a) Fig (b) Fig(c) Fig (d)

Fig (a, b, c, and d) shows the Encryption process at the Bank's Server side



Decrypt the Text

9958c656bdab81beed1d30d0dc0
7d04ba006d12d4f204a75

Enter key to decrypt

1a%r1a

One Time Password

Your password is 642139

Fig (e) Fig (f) Fig (g)

Fig (e, f, and g) shows the Decryption process at the User's side

IV. Conclusion and Future work

Internet banking is offering its customers with a wide range of services: Customers are able to interact with their banking accounts as well as make financial transactions from virtually anywhere without time restrictions. In order for electronic banking to continue to grow, the security and the privacy aspects need to be improved. With the security and privacy issues resolved, the future of electronic banking can be very prosperous. The future of electronic banking will be a system where users are able to interact with their banks "worry-free" and banks are operated under one common standard. The security models for online banking systems currently in use are strongly based on Internet banking user identification and authentication methods, which are also the components where most Internet banking systems' vulnerabilities are found.

This paper describes current online banking problems and discusses the need for security testing for online banking. The system allows user to carry out all banking transaction securely from anywhere, anytime. We have implemented system using symmetric key IDEA algorithm.

In future better power consumption algorithm like blowfish can be tried out. Steganogrpahy can also be applied for secure Internet banking and mobile banking transactions. We can use concept of STK, SIM application toolkit where bank can stored the application and encryption keys on SIM.

REFERENCES

[1] Sandeep Singh Ghotra, Baldev Kumar Mandhan, Sam Shang Chun Wei, Yi Song, Chris Steketee, "*Secure Display and Secure Transactions Using a Handset*", Sixth International Conference on the Management of Mobile Business.

[2] Dilla Salama Abdul Minaam. Hatem M. Abdul Kadir, Mohily Mohamed Hadhoud*," Evaluating the effects of Symmetric Cryptographic algorithms on Power Consumption for different data types*", International Journal of Network Security, Volume 11, September 2010.

[3] Managing the Risk of Mobile Banking Technologies, Bankable Frontier Associates.

[4] Richard E. Smith. Authentication: From Passwords to Public Keys. Addison Wesley, 2001.

[5] Encryption Issues. Http://www.muc.edu:80/cwis/person/student/lockett/encryption.html

[6] Internet Security. Http://cfn.cs.dal.ca/Education/CGA/netsec.html

[7] MICROSOFT, An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software, focusing on the first half of 2008 [Report]. Security Intelligence Report, January through June 2008.

[8] M. JOHNSON, A new approach to Internet banking. University Cambridge. (PhD) 2008, p. 113.

[9] Carneiro, B. and Sousa, R. T., Identifying Bank Frauds Using Crisp-DM and Decision Trees,
International Journal of Computer Science & Information Technology. October, vol. 2, 2010, pp. 162 - 169.

[10] Development, Why is J2ME MIDP superior to WAP, http://www.developnet.co.uk/wap.htm.

[11] Laitinen, H., 2001, Sun's 2001 Worldwide Java Developer Conference, Development Tools for the J2ME, http://www.forum.nokia.com/main/1,35452,1_0_75,00.html.

[12] Java 2 Platform, Micro Edition – J2ME, Official Site, http://java.sun.com/javame/index.jsp.

[13] CEM, "Common Criteria for Information Technology Security Evaluation", version3.1, 2006. [Online]. Available:http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R2.pdf

[14] A. Hiltgen.; T. Kramp; T. Weigold; "Secure Internet-banking Authentication," *IEEE Security and Privacy*, vol. 4, no. 2, 2006, p.21-29.

[15] F. Puente; J.D. Sandoval; P. Hernandez; C.J. Molina; "Improving online banking security with hardware devices", *39th Annual 2005* International Carnahan Conference on Security Technology *(CCST'05),* 2005. 11-14 Oct. 2005 pp.174 – 177.

[16] Testing Verification and Validation Workshop*, 2008. ICSTW apos; 08*. IEEE International Conference, 9-11 April 2008 pp. 294 – 302.

[17] K.Chikomo, M.K. Chong, A. Arnab, A. Hutchison (2006), "Security of mobile banking", University of Cape Town, South Africa, Tech. Rep. [Online]. Available: http://pubs. cs.uct.ac.za/archive/ 00000341/01/Security of Mobile Banking paper.pdf.

[18] A. Shamir, "Identity-based cryptosystems and signature schemes", in CRYPTO: Proceedings of Crypto, 1994.

[19] N. Croft, M. Olivier, "Using an approximated One-Time Pad to Secure Short Messaging Service (SMS)", in Proceedings of the Southern African Telecommunication Networks and
Applications Conference (SATNAC), 2005, pp. 71–76.

[20] Sun Microsystems Wireless Toolkit http://java.sun.com/products/j2mewtoolkit

[21] Bouncy Castle http://www.bouncycastle.org/

[22] ProGuard http://proguard.sourceforge.net/

[23] Computer security http://searchsecurity.techtarget.com/