International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 7, July 2014

Framework for Secure Mobile Banking Application Using Elliptic Curve Cryptography & Image Steganography

J. Saranya [1], S. Thirumal[2]

[1]M.Phil research Scholar A.A.A. Govt .Arts College, Cheyyar, T.V. Malai Dt, India

[2]Assistant Professor & Head, of Computer Science, A.A.A govt. Arts College, Cheyyar, T.V. Malai Dt, India

Abstract: ***The Wide-expansion of mobile telecommunication technology mobile banking emerged as a new type of financial services and can provide efficient and effective financial services for clients. Mobile banking is a way for the customer to perform banking actions on his or her cell phone or other mobile device. It is a quite popular method of banking that fits in well with a busy, technologically oriented lifestyle. Framework conditions for mobile banking services differ from country to country but one thing is certain: the future of mobile banking depends on getting the security right. In this paper, we present a new way of securing mobile banking. We introduce a system which makes use of Elliptic curve cryptography and RGB Intensity Based Randomized pixels with variable Bits image Steganography [5]. Elliptic Curve Cryptography suites well for resources constraint devices like mobile phones and PDA, because of its less computation time, short key's length, fast digital signature, flexibility and less resource consumption.***

Keywords: Mobile banking, Elliptic curve cryptography, Steganography, Trusted server

1. Introduction

Mobile Banking scores over Internet Banking because it enables 'Anywhere Anytime Banking' and also it reduces the customer requirement to just a mobile phone. The biggest advantage Mobile Banking provides to the banks is that it helps to cut down the costs as it's even more economic than providing tele-banking facilities where banks have to keep hundreds of tele-callers. Additionally, Mobile Banking helps banks to upgrade the quality of services and nature of customer relationship management But Security concerns are the single biggest factor inhibiting consumer acceptance of mobile banking. The rest of the paper is organized as follows. Section 2 discusses our proposed system. Section 3 represents results of the proposed system. Finally, section 4 discusses the conclusion and future work.

2. Related Works

The most popular type of mobile banking is Short Message Service (SMS). The advantages of using SMS are that it is relatively inexpensive and it is reliable for sending non-sensitive messages. SMS messages are sent asynchronously. When a message is submitted for sending, the service provider will keep the sending message in its message buffer until the message is delivered to the destination mobile phone. The problems with SMS banking are that the SMS message is not entirely secured. There are many flaws in the GSM architecture which lead to security shortfalls for SMS banking. In USSD mobile banking the verification depends only on the sender's number, such that if the SIM card is lost or the SIM card is duplicated, the attacker can use the victim's account to perform transaction and also the USSD message that gets sent to the bank server is only encrypted between the mobile station and the base transceiver station. The message is in plaintext within the mobile operator's network.

3. Proposed System

In this proposed solution, Elliptic curve cryptography is used which provides high-level security. On the other hand, to improve the security of data send from bank server to client, The overview of the proposed system is described in the image based Steganography is used.

A. System overview

The overview of the proposed system is described in the following section Fig.2. provides brief understanding about the complete system. The system is comprised of four major components. The components are Trusted Server (T), Client application (C), Bank Application Server (B) and Bank Database. When bank customer starts the application C, both C and B, receives secure data dynamically from T to generate the session key. The customer provided banking details are sign crypted to generate secure SMS packet based on message format specified in fig.1and send to B via GSM network. In B, if received SMS is intended for banking unsign cryption takes place. Otherwise SMS packet is discarded. Then B, process the requested service and requested service info is sign crypted. Based on clientid SMS/MMS packet is generated. If client ID is '1' then sign crypted data is hidden into an image to generate MMS or else SMS is generated. And generated SMS/MMS is send to C via GSM network. In C, signed message is extracted from received MMS image or obtained from received SMS. If unsign cryption succeeds then service details are shown to the bank customer. Otherwise received SMS/MMS packet is discarded.

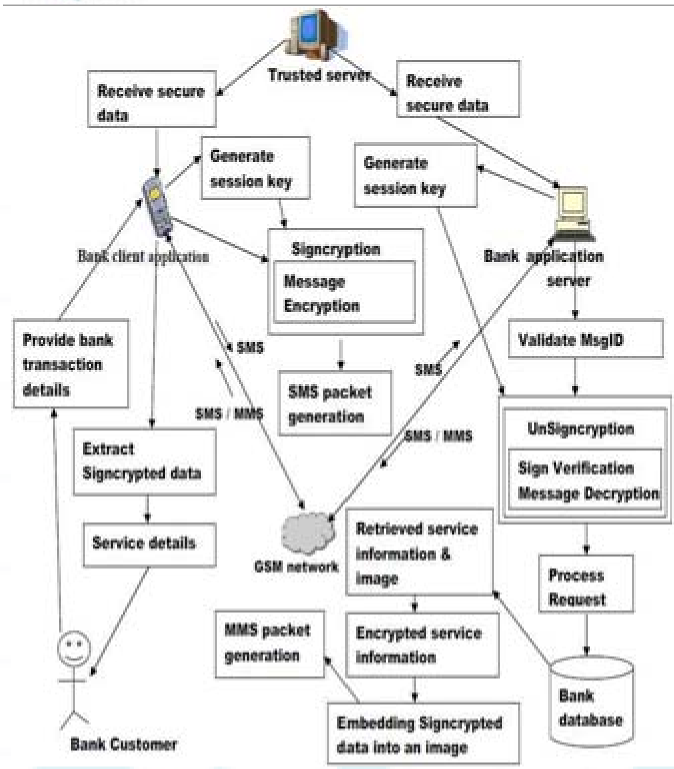

Figure 2: System Architecture

B. Pseudocode

The pseudocode for the algorithms are discussed in the following section,
a. Three party key agreement protocol using ECC
b. Signcryption scheme
c. RGB intensity based Randomized pixels with variable bits image Steganography

Table 1: The notations used in algorithm

$E(F_p)$	Elliptic curve over finite field F_p
AES	Advanced Encryption Standard
$Encrypt_{skey}()$	AES Encryption function
$Decrpt_{skey}()$	AES Decryption function
ID_c ID_b	Identity of Client and Bank server
Z	Secret Octet string
H	One way Hash function
KDF	Output of Key Derivation Function
EM	Shared symmetric key
DM	Tag for encrypted message
pow	Logarithm of order 'n'
||	Concatenation operation

C. Three party key agreement protocol using ECC:

This protocol is used to obtain a session key which is used in signcryption scheme. It involves 2 phases, one is assignment phase and other is key exchange phase [5]. Assignment phase: In this phase, all the three parties C, B and T are agreed upon certain parameters, which are described in the following steps.

Step 1: Select prime finite F and check $p>2^{192}$
Step2: Choose the field element 'a' and 'b' which satisfies $4a^3+27b^2\neq0$(mod p) and select base point G of order n
Step3: Publish E (F_p), Encrypt ( ), $Decrpt_{skey}$ ( ) and G.

Step4: Bank customer C and bank application server B register to trusted server T. Then C, B and T generates private|public key pairs d $|U_c$, $d_b|U$, and $d_t|U_t$ respectively $U_c=d_c*G$, $U_b=d_b*G$, $U_t=d_t*G$ where *represents point multiplication.
Step5: Select U_a, a secure point known only to customer and bank server and it differs for each customer.

Key exchange phase: In this phase, here C and B, exchange some parameters through T, that parameter will be used for generating session key .This phase is further subdivided into three Subphases.

Subphases1 Client application(C)
Step1: Calculate K $= d_c *U_t = (K_{cx},K_{cy})$
Step2: Compute EC_c = Encrypt (ID_b)
K_{cx} and K_{cy} are x and y coordinates of K_c
Step3: Send (ID_c ,EC_c) to T.

Subphases 2 Trusted server(T)
Step1: Receive (ID_c ,EC_c) from customer
Compute K $=d *U_c =(K \ ,K_{cy})$
Compute PT_c =Decrypt (EC_c)
Step 2: If Decryption Succeeds , then goto Step3 Otherwise, T sends an authentication failure message to C
Step3: Compute K $=d *U_b=(K_{bx},K_{by})$
Generate an random number r € $E(F_p)$
Step 4: Compute ECtc=Encrypt (r) and
EC_{tb} =Encrypt (r,ID_c)
Step 5:T send EC_{tc} to C and EC_{tb} to B.

Subphases 3 Session Key Generation
Step1: C receives EC_{tc} and B receives EC_{tb} from T
Step2: C compute K = $d_c *U_t = (K_{cx},K_{cy})$ and B computes K $=d *U_t=(K_{bx},K_{by})$
Step3: Both C and B decrypts the received EC_{tc} and EC_{tb} using the keys K_{cx} and K_{bx} respectively.
Then C computes r= Decrypt (EC_{tc}) and
B computes r=Decrypt (EC_{tb})
Step4: Both C and B calculates $SK=U_a*r$ SK=(SK , SK)
where SK represents session key

D. Signcryption scheme

In the signcryption scheme it involves two phases[3],one is to generate the signed message and other is to verify signed message. The proposed scheme references the existing scheme[3] and the modified steps are highlighted bold in both the phases. Signcrypted text generation phase: In this phase, message is encrypted using (AES) encryption algorithm [3], it uses session shared symmetric key (EM) and for the encrypted message, sign is generated using private keys dc and db for C and B respectively.

Step1: Select random integer r_{as} € $E(F_p)$
Step2: Compute $R_s=r_{as}$ * G where $R_s=(R_{sx},R_{sy})$
Step3: Compute $K_s=(r_{as}+ \quad * d_c)* U_b$
$Rsx= 2^{(pow/2)}+ (R_{sx} \bmod 2^{(pow/2)})$

International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 7, July 2014

Step4: Check K_s=0, if K_s=0 go to step1 else Compute $Z=H(K_{sx} ||ID_c||SK_x ||K_{sy}||ID_b)$
Step5: Compute KDF=H(Z||Counter) where
KDF=EM||DM
CT=Encrypt (M)
Step7:Compute $x=H(CT||R_{sx}||ID_c||DM||R_{sy}||ID_b)$ and Compute digital signature $S=x*d_c - r_{as}$ (mod n)
Step8: Send signcrypted text (R_s,CT,S)

Unsigncryption phase: In this phase, for the received signcrypted message, sign is verified using public keys U_c and U_b for C and B respectively. If sign verification succeeds, then encrypted message is decrypted using AES decryption algorithm. Otherwise message is discarded.

Step1: Compute $K_s=d_b(R_s+ \quad *U_c)=(K_{sx},K_{sy})$
Step2: Compute $Z= H(K_{sx}||ID_c||SK_x||K_{sy}||ID_b)$
Step3: Compute KDF=H(Z||counter)
Step4: Compute $x=H(CT||R_{sx}||ID_c||DM||R_{sy}||ID_b)$
Step 5: If $S*G+R_s=x*U_c$ then accepts CT to decrypt, Otherwise Rejects CT
Step 6: Decrypt the encrypted message CT and plain text M=Decrypt (CT)

E. RGB Intensity based Randomized pixels with variable bits image steganography algorithm

This algorithm hides data inside an image based on Intensity of RGB channels and partition scheme [4]. To hide the data, random pixels are chosen based on Ua. For generating indicator sequence and for selecting partition scheme ‘r’ is used, which is sent by T.

Embedding phase:
Step1: Generate an Indicator Sequence from ‘r.
Step 2: Select random pixels based on ‘Ua’
Step 3: Generate partition scheme based on ‘r’ Choose number of data bits to store based on partition scheme and channel value
Step 4: Store the data bits
Step 5: Modify the other channel ‘s LSB, which is used while retrieving the data.
Extraction phase:
Step1: Generate an Indicator Sequence from ‘r’
Step 2: Select random pixels based on ‘Ua’
Step 3: Determine the channel hiding data by checking LSB of two channels in a pixel other than a indicator
Step 4: Determine number of data bits hidden in the above determined channel based on partition scheme.
Step 5: Read the data bits

4. Results

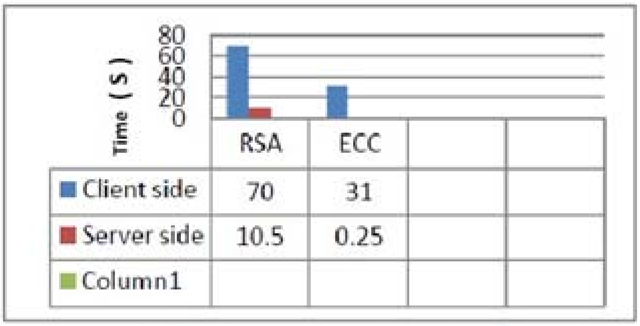

Figure 3: Algorithms time taken

The proposed system overcomes the security shortfalls in the existing system [1]. The proposed system provides security services such as availability, mutual authentication, non-repudiation, data integrity. The cost of each transaction in proposed system is less, when compared to GPRS banking. The minimum number of SMS required to perform a single transaction is two. The embedding capacity of the image (124 X 124) pixels is 30 times greater than the size of SMS packet. There are no major variations in the histogram of the image after data is embedded into it.

5. Conclusion & Future Work

In this paper, we have first presented the background of mobile banking system and follows design, implementation & results of a proposed system. The future works relates to the secure m-payments. Our proposed system acts as an initiative to MMS banking. In the near future, whole mobile banking system is transferred from partial MMS banking to complete MMS banking depending on mobile phones.

References

[1] M. Shirali Shahreza, "An Improved Method for Steganography on Mobile Phone", WSEAS Transactions on Systems, Issue 7, vol. 4, pp. 955-957, July, 2005.
[2] D. Hankerson, A. Menezes, and Scott Vanstone, “Guide to Elliptic Curve Cryptography,” Springer-Verlag, New York, 2004.
[3] M. Toorani, and A.A. Beheshti Shirazi “A Directly Public Verifiable Signcryption Scheme based on Elliptic Curves”
[4] Mohammad Tanvir Parvez and Adnan Abdul- Aziz Gutub “RGB Intensity Based Variable-Bits Image Steganography” 2008 IEEE Asia-Pacific Services Computing Conference
[5] Jen-Ho Yang , Chin-Chen Chang “An efficient three-party authenticated key exchange protocol using elliptic curve cryptography for mobile- commerce environments”, The Journal of Systems and Software (2009).