ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

OTP Encryption Techniques in Mobiles for Authentication and Transaction Security

Dr.AnanthiShesashaayee, D. Sumathy

Associate Professor & Head, Department of Computer Science, Quaid E Millath Government College for Women, Chennai, Tamil Nadu, India

Research Scholar, Department of Computer Science, Quaid E Millath Government College for Women, Chennai, Tamil Nadu, India

A**BSTRACT**: The improvement and advancement in technology makes the modern day smart phones and PDAs moresophisticated .It has drastically changed the way in which we perform our m-banking transactions. When a client initiates a bank transaction, he is provided with an OTP which is sent to his registeredmobile number via SMS. The client sends back the OTP within a short period to complete the transaction. The OTP SMS is generated by the bank server and is handed over to the client's mobile operator. To avoid any possible attacks like phishing, man-in-the-middle attack, malware Trojans, the OTP must be secured. In order to provide a reliable and secure mode of online transactions without any compromise to convenience, a reliable m-banking authentication scheme that combines the secret PIN with encryption of the one-time password (OTP) has been developed in this paper. The secret PIN known only between the client and the bank is used for encrypting the OTP. After the encrypted OTP SMS reaches the client's mobile, the PIN is used again used for decrypting. The plain OTP text should be sent back to the bank will verified at the server to complete the transaction initiated. The combination of PIN with OTP provides authentication and security. The proposed scheme provides security even if any disputes arise due any possible attacks like internet hacking or mobile thefts.

KEYWORDS: M-banking, Phishing, Malware Trojans, User authentication, One-Time Password, PIN, Fiestal network

I. INTRODUCTION

Electronic commerce (EC) is a term used to perform any kind of business or commercial transactions with the help of internet. It provided services like on-line shopping, E-trading, E-banking, on-line services like travel tickets booking, e-tickets etc. An online transaction system is a payment method that authorizes transfer of funds over an Electronic Fund Transfer (EFT). Even in developing countries people prefer online payments because of the convenience and costs. In online transactions, the electronic payments are made through credit cards/debits cards or direct net banking transactions. E-payments are the most preferred mode for any transactions because of the safety and security features it possess. E-payments have become an indispensable mode and are increasingly used everywhere from small merchants to big, to conduct business. Online payments simplify our lives to a greatextent [1].

Electronic banking (e-banking) is one of the most successful businesses of e-commerce. The customer is free conduct business without any spatial and temporal limitations. Banks uses e-banking because this not only satisfy the customer needs but also possess more economic advantage by replacing the highly paid bank clerks with central web server which costs much less. With the advancement and improvement in technology, more sophisticated smartphones and PDAs have become more popular. Since people consider that cellular phone is a personal dependable tool and it is becoming the essential thing of their lives. This has made a drastic change in how we perform our bank operations. Almost all the devices are capable of using internet,cellular phones was the subsequent move in the development of electronic banking. [7]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

II. RELATED LITERATURE

A. *M-Banking.*

SMS banking is a type of mobile banking, a technology-enabled service offering from banks to its customers, permitting them to operate selected banking services over their mobile phones using SMS messaging. Mobile banking services consists of information inquiry, notifications and alerts, applications and payment transfer. [11]. Mobile banking (M-banking) has more advantages than the electronic banking: these devices can be accessed at anytime and anywhere, mobile devices provides more security than personal computers. Even banks are hiring comparativelyless number of clerks as m-banking has gained so much popularity. The income and loss account is moreover favourable: for instance bank transaction via clerks costs very more than a bank transaction using mobile banking application [7].
The user is given the privilege of accessing their account for Debit/Credit card information with a single SMS. Using SMS banking, the account balance can checked, account summary can be viewed, reward points can be checked, requests for cheque book, withholding payment against an issued cheque can be done. Generating transaction alerts over important events like credit of a cheque, debit of balance, credit/debit transactions for amount more than a specified amount, dishonoured cheque, and lack of minimum account balance are some of the Push services provided through mobiles instantly. Any access to the customer's bank account for online payment transfers, entry into the profile section of the customer will immediately communicated through SMS and need to be authenticated using **OTP (One Time Password)** received at the customer's mobile before proceeding with the transaction. SMS alerts on unauthorized accesses to bank accounts, fraudulent transactions etc. are sent immediately to the customers. Mobile based application is used for connecting customer handset with bank server for all such services**.** Banks checks the authenticity of the user before any Pull services can proceed. The user's mobile number must be registered with the home branch of the bank, in person, in which the customer has account. The bank, for any transaction or enquiry requested, checks the genuinely of the person and also the transaction initiated is approved, before proceeding using an SMS to the registered mobile number.[11]

B. *One-Time Password-Mobile Transaction Authorization Number.*

One Time Passwords.(OTP) are utilized as an additional factor in multi-factorauthorization/authentication applications. They are only valid for exactly oneauthorization or authentication request. To avoid password lists, a convenientway to provide the user with an OTP is to send it via SMS. The phone number ofthe user must be registered for the service that provides SMS OTPs for authenticationor authorization. OTPs are quite

popular as an additional authorization orauthentication factor in web-based services.[2]

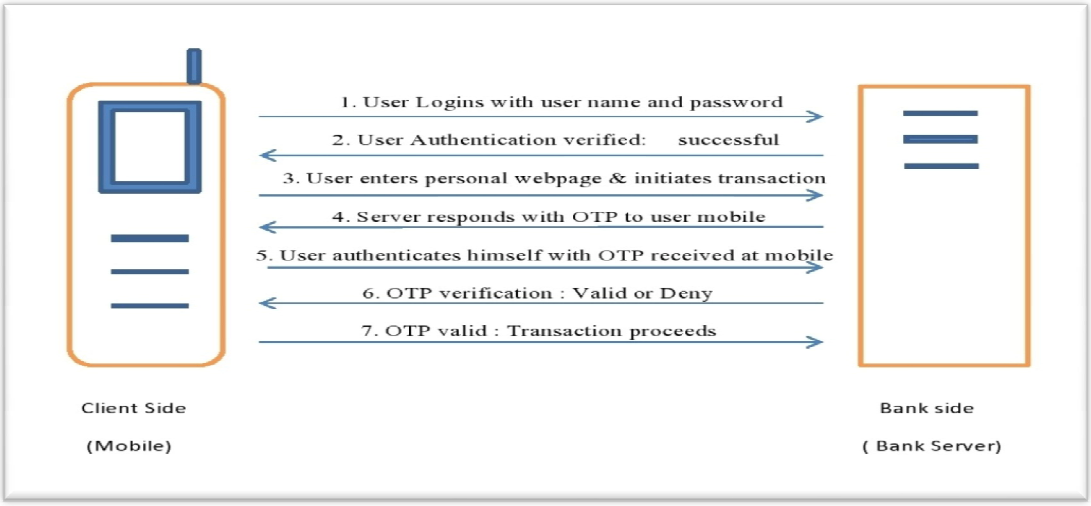

Figure 1.OTP generation and User authentication

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

The traditional method of generating OTP whenever the user initiates a banking transaction is as follows. In the first step the user enters the home page of the bank in which he has his account. He then enters his user name and password. He is allowed to login into his webpage of his personal account,if the user authentication is valid. The user then initiates a transaction and the bank server responds back with OTP also called as [2]mobile Transaction Authorization Number(mobile TAN or mTAN) to his mobile or PDAs. This is the second level of authentication done to avoid password thefts. The user then authenticates with OTP himself with OTP. The OTP is checked at the server and the transaction proceeds if valid.

There are two main approaches to OTP [5]. In the first approach, called time-based OTP, theone-time password changes at frequent intervals (say, every two minutes). In the secondapproach, called event-based OTP, the one-time password is generated for every transaction or login from a different IP address.

C. *Threats to OTP*.

(i) Wireless Interception:

The GSM technology is insecure due to several vulnerabilities such as a lack of mutual authentication and weak encryption algorithms. Further research shows that the communication between mobile phones and base stations can be eavesdropped and decrypted using protocol weaknesses. Lately, it has been shown that femtocells (small 3G base stations that are deployed in user homes) can be abused to intercept 3G communication, including SMS messages [2].

(ii) Mobile Phones Trojans:

Mobile phone malware, and especially Trojans, that are designed to intercept SMS messages containing OTPs, are a rising threat. This kind of malware is created by criminals directly for the purpose of making money. In the following, we provide an overview of the different kinds of SMS OTP stealing Trojans. The ZITMO (Zeus In TheMObile) Trojan for Symbian OS is the first known piece of malware that was specifically created for interceptingmTANs. ZITMO can also delete SMS messages. This capability can be used to completely hide the fact that an SMS messagecontaining an mTAN ever arrived at the infected phone. Further, the ZITMOTrojan can be remotely reconfigured via SMS. Through this the attacker can,for example, change the destination number for forwarded SMS messages. This Trojan buys items from online stores and intercepts the SMS messages containing a verification code that isneeded to complete the payment process. Additionally, further mobile malware,also steals authentication credentials, and attacks mobile phone owners [2].

A new commercial mobile phone Trojan ***mSpy*** is a mobileapp that can be installed on the phone to be hacked. Once installed, universal remote access can be gained to the monitored mobile and able to read their texts any time as and when needed. With ***mSpy***installed, all the calls to that mobile can be monitored, text messages can be tracked, e-mails synchronized to the mobiles can be read, GPS location can be tracked, Calendars and address books can be accessed and instant messages can be read. It transfers hacked data in small packets so that it is not obvious and can almost never be detected.[10]

(iii) Phishing

Phishing is a form of electronic identity theft in which a combination of social engineering and web site spoofingtechniques are used to trick a user into revealing confidential information with economic value. In a typical attack, theattacker sends a large number of spoofed e-mails to random internet users that appear to be coming from a legitimatebusiness organization such as a bank. The e-mail urges the recipient (i.e., the potential victim) to update his personalinformation using links in the email, if the recipient does not do so it will result in the suspending of his online banking account. Such un-grounded threats are common in social engineering attacks and are an effective technique inpersuading users. When the unsuspecting victim follows the phishing link provided in the e-mail, he is directed to a web site that is under the control of the attacker. The site is prepared in a way such that it looks familiar to the victim by imitating the visual corporate identity of the target organization by using same icons, logos and textual information. [1]

a.Visually deceptive text: Users may be fooled by the syntax of a domain name in “type jacking” attacks, which substitute letters that may go unnoticed (e.g. www.paypai.com uses a lowercase “i” which lookssimilar to the letter “l”, and www.paypa1.com substitutes the number “1” for the letter “l”.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

b.Images masking underlying text: One common technique used by phishers is to use an image of a legitimate hyperlink. The image itself serves as a hyperlink to a different, rogue site.

c. Windows masking underlying windows: A common phishing technique is to place an illegitimate browserwindow on top of, or next to, a legitimate window. If theyhave the same look and feel, users may mistakenlybelieve that both windows are from the same source,regardless of variations in address or security indicators. [1]

(iv) Man-In-The-Browser

An MITB attack is essentially a man-in-the middle (MITM) attack, but unlike typical MITM attacks, which usually occur at the protocol layer, MITB attacks are introduced between the user and browser. Malware, especially Trojans, is used to infect the browser. The malware is normally installed when a user clicks on an applet on a web site that he/she is duped into clickingbecause it claims that an update or other similar action is needed. MITB malware is mostly undetectable by current antivirus software, although it may be detected if protection levels are set very high, which would also inhibit many innocuous programs. MITB modifies a user's content when an online banking site is visited by adding extra fields to the page in order to compromise second authentication mechanisms. In an MITB attack, the customer initiates a transaction, the attacker modifies the transaction using compromised credentials, the extra fields added by the malware alert the attacker and give the hacker control of the online banking interface, consequently manipulating the statement and account balance to reflect the customer's intended transaction. Once the user uses a token to generate an OTP or receives it in a text message, the user enters the code and unknowingly authorizes the manipulated transaction thinking it was the correct one. [8]

(v) Password Stealing and Identity Theft:

The user name and the password can be stolen by shoulder-surfing and by guessing. These kinds of attacks happen normally by a person of close association. Human tendency is to have passwords with their birthdates or their favorites, something that is easy to remember. This makes the fraudsterseasy to guess and do the unauthorized transactions.

A malware based attack,ZeuS, infects the user mobiles and sniff all SMS that are being delivered to the infected mobile. The attacker steals both user name and password using the malware. The attacker then forces the user to install a malicious mobile application by luring him with some innocent piece of code .The attacker then logs on with stolen credentials. When the OTP is sent to the user mobile for authentication, the malicious software forwards the OTP SMS to the terminal controlled by the attacker. The attacker then enters the OTP and completes the bankingtransaction.[13]

III. RELATED TECHNIQUES FOR SECURING OTP

Protecting the OTP from the various malwares, MITB attacks various ideas were suggested.

A. *SMS End-to-End Encryption:*

The first idea use end-to-end encryption to protect OTP messages when theSMS message gets intercepted or eavesdropped on. The OTP generated is encrypted using the powerful AES algorithm. The generated OTP value is encrypted using powerful AES algorithm and sends it to users.AES is an iterative and asymmetric key block cipher that uses three keys strengths of 128, 192 and 256 bits. The AES uses 128 bits as a block for encryption and decryption. bits. It is one of the perfect cryptography algorithms to protect personal data. The encrypt AES tool converts the input plain text to cipher text in a number of repetitionsbased on the encryption key. The AES decrypt method uses the same process to transform thecipher text back to the original plain text using the same encryption key. It is very difficult to break even using brute force attack. The encrypted OPT password is send to mobile through Bluetooth technology or modem[13]. The drawback of this method is that it has large system load for encryption and decryption.

B. *Virtual Dedicated channel on the Handset:*

The mobile Trojans are a major threat to the SMS OTP. A virtual dedicated channel is created to protect against Trojan attacks that requires minimal supportfrom operating system manufacturers and minimal-to-no support from theservice provider and cellular network operators. This dedicated channel *inside the mobile phone OS* by removing *certain* SMS messages from thegeneral delivery process on the phone and redirecting them to a special OTPapplication.The endpoint of the virtual dedicated channel is an applicationwith similar functionality to the default SMS application. It receives

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

and storesSMS messages. The only difference is that it will only receive OTP messages,and that its message store cannot be read by other applications.[2]. The server should distinguish the confidential messages from the normal ones.

IV.PROPOSED METHODOLOGY FOR SECURING ONE TIME PASSWORD USING FEISTAL NETWORK

In this paper, Feistal Network method of encryption is proposed for ciphering OTP. The main advantage of this method is that the size of the input can be easily changed .The sub-keys are generated in each round and this produces cascading iterations. It becomes difficult to crack if more rounds are used for encryption.

Encryption Phase

Let F be the round function and let K_0, K_1 …,K_{n-1}be the sub-keys for the rounds 1,2,..,*n* respectively.
Then the encryption operation is as follows:

(i) Split the plaintext block into two equal pieces, (L_0, R_0)

(ii) For each round $i = 0,1,2,\ldots,n$, compute

(a) $L_{i+1} = R_i$

(b) $R_{i+1} = Li \oplus F(R_i, K_i)$

(iii) Then the cipher text is (R_{n+1}, L_{n+1}).

(iv)

Decryption Phase

The decryption of the ciphertext (R_{n+1}, L_{n+1}). is accomplished by computing the same round function F, for $i = n,n-1,\ldots,0$ and the reversal of the sub-keysK_n ,K_{n-1} …,0

(v) $R_i = L_{i+1}$

(vi) $L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$

(vii) Then (R_0, L_0) is the plain text again.

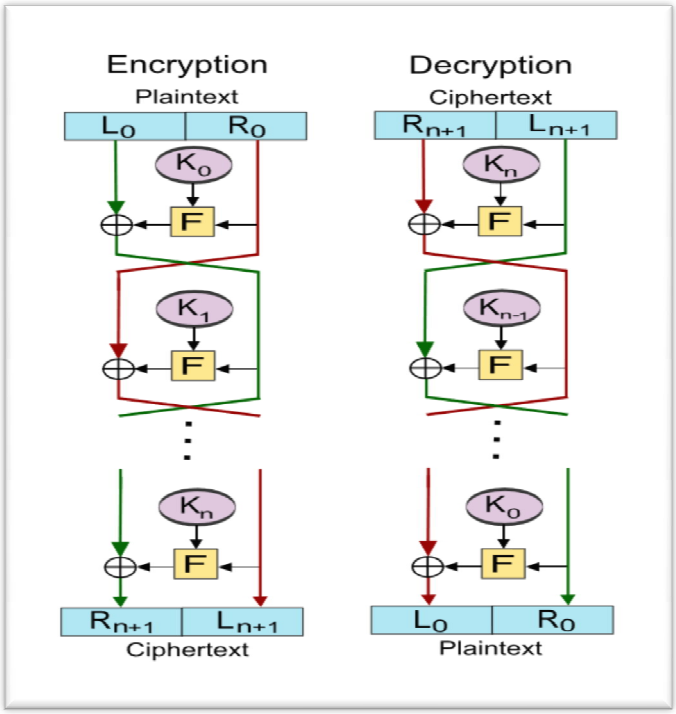

Figure 2.Feistal Network for encryption and decryption [12]

When the user logins with user name and password and initiates a bank transaction the bank server generates a random six-digit OTP. This OTP is transmitted via the communication channel as SMS to the user mobile. In the proposed

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

method for enhancing the security of OTP or mTAN, the server encrypts the OTP instead sending it as plain text to the user mobile.

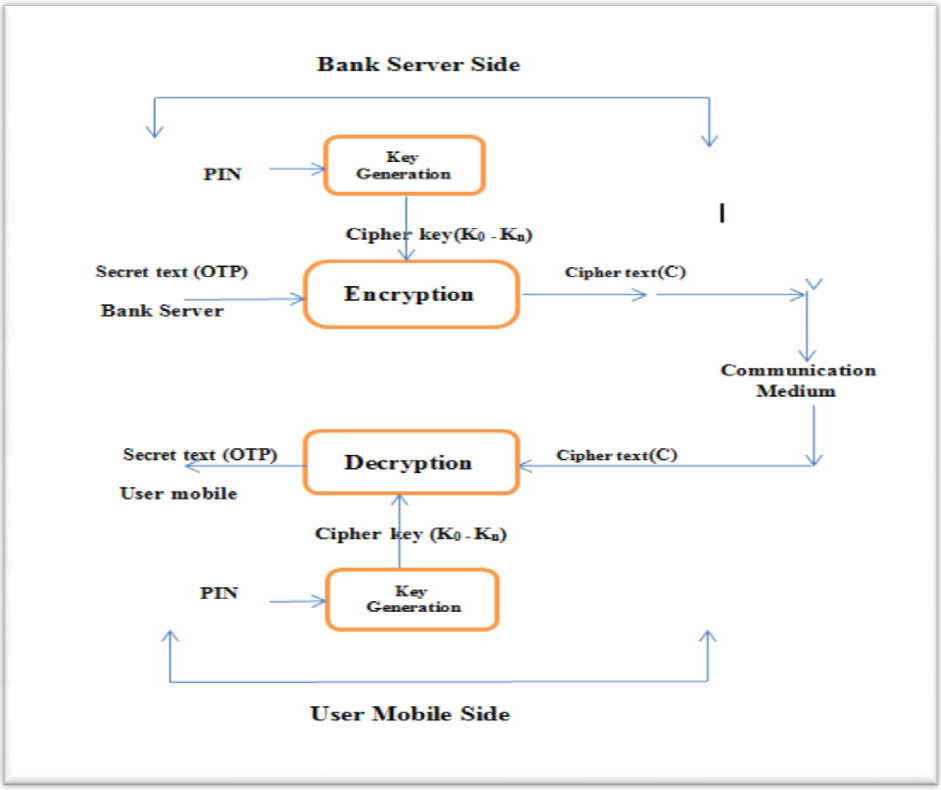

Figure 3.Proposed idea of OTP encryption

A 4-digitsecret Personal Index Number (PIN) is given by the banks, when the user is registered for internet banking/mobile banking. This is stored at the server and acts as a tool for generation of sub-keys for the different rounds of feistal network whenever a particular user initiates a transaction

.**Step I. Key Generation at the Server.**

(i) The user is provided with a 4-digit PIN by the banks (like 5639). The pin is unique and a secret for every user.

(ii) The digits of the PIN are added. Say ***p.*** (here. 5+6+3+9= 23, 2+3=5).

(iii) Now, ***p*** mod ***q*** = ***n***. Here ***q*** is a number chosen by the bank for an individual user.

For example,

PIN = 5639

p = 5

(iv) 5 mod 3 = **2**

(v) This PIN is binary coded individually. 0101 0110 0011 1001. These digits can be stretched by adding **2** to every digit.

(vi) The binary coded stretched keys are

0101 0111 0110 1000 0011 0101 1001 1011

(K_0) (K_1) (K_2) (K_3)(K_4) (K_5) (K_6) (K_7) (no. of rounds = 8)

This key K_0 – K_7, is used as the sub-keys for the individual rounds of the feistel network. These are stored in the bank server and used every time the particular user initiates a transaction**.**Here the secret PIN and ***q***are unique for every user who registers with the bank for m-banking transactions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Step II: Encryption using Fiestal Network:

The input to the fiestal network is the data block and the key. The input is divided into two halves and with the sub key generated using PIN,the data is iterated through a number of rounds. The inputhere is the 6 digit binary coded OTP and the sub keys areK_1,$K_{2...}K_7$for each of the 8 rounds.

OTP : 463967

OTP in BCD form : 010001100011100101100111

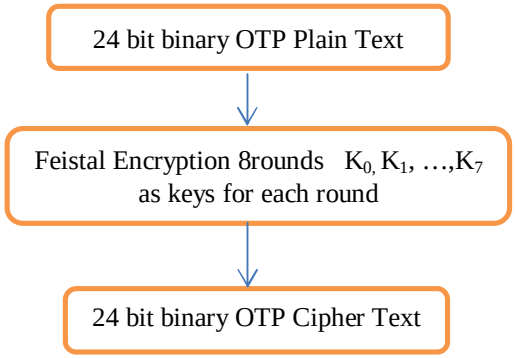

Figure 4.OTP Feistal Cipher Encryption.

There are many rounds in fiestal method of encryption based on the number of keys. In each round, the plain text undergoes some transformation based on the sub keys for each round..

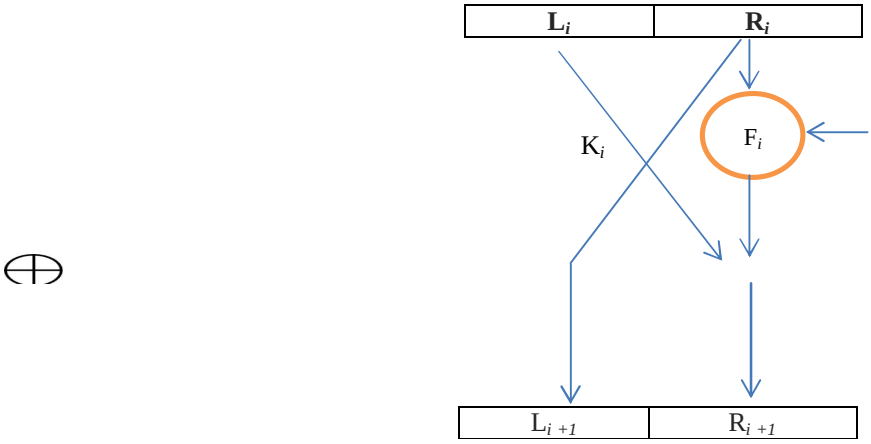

Figure 5. Single round of feistal network

L_0 and R_o - Input for Round 1 , the initial values for entering into the network.

$L_i$and R_i - Output for Round *i*

F_i - Round function *i*

K_i - Sub key for round *i*

For each round $i = 1,2,\ldots,n$, compute

$L_{i+1} = R_i$

$R_{i+1} = Li \oplus F(R_i, K_i)$

The cipher text after encryption phase is (R_{n+1}, L_{n+1}).

010001100011	100101100111
L_0	R_0

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Round I

$L_1 = R_0$

$R_1 = L_0 \oplus F(R_0 , K_0)$

R_0 = 1001 0110 0111

K_0= 0101 0101 0101

F_0 = 1100 0011 0010

L_0 = 0100 0110 0011

R_1 = 1000 0101 0001

100101100111	100001010001
L_1	R_1

o

o

o

Round VIII

$L_8 = R_7$

$R_8 = L_7 \oplus F(R_7 , K_7)$

R_7= 1010 0111 0011

K_7 = 1011 1011 1011

F_7 = 0001 1100 1000

L_7 = 1110 0001 0000

R_8 = 1111 1101 1000

101001110011	111111011000
L_8	R_8

The cipher text is101001110011111111011000

This cipher text travels through the communication medium and reaches the user mobile.

Step III : Key Generation at the Mobile.

The encrypted binary OTP is stored at the inbox of the user mobile. The user is requested to enter the PIN and the sub keys K_1, $K_{2...}$ $K_7$are generated by the same technique as done at the server. These sub keys are passed to the decryption phase for generating 24 bit OTP plain text.

Step IV: Decryption using Fiestal Network:

101001110011	111111011000
L_8	R_8

$R_i = L_{i+1}$

$L_i = R_{i+1} \oplus F(L_{i+1},K_i)$

Round I

$R_7 = L_8$

$L_7 = R_8 \oplus F(L_8,K_7)$

L_8 = 1010 0111 0011

K_7 = 1011 1011 1011

F_8 = 0001 1100 1000

R_8 = 1111 1101 1000

L_7 = 1110 0001 0000

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

111000010000	101001110011
L_7	R_7

o

o

o

Round VIII

$R_0 = L_1$

$L_0 = R_1 \oplus F(L_1, K_0)$

$L_1 =$ 1001 0110 0111

$K_0 =$ 0101 0101 0101

$F_1 =$ 1100 0011 0010

$R_1 =$ 1000 0101 0001

$L_0 =$ 0100 0110 0011

010001100011	100101100111
L_0	R_0

Plain Text: $L_0 R_0$

010001100011	100101100111
L_0	R_0

OTP in BCD form : 0100 0110 00111001 0110 0111

OTP : 463967

The ciphered OTP can be decrypted only if the 4 digit PIN entered by the user at his mobile is correct. Since the PIN is known only to the user, even if the hacker sees the encrypted OTP, it cannot be decrypted.

Step V:Two-tier User Authentication with PIN and OTP.

The ciphered OTP can be decrypted only if the 4 digit PIN entered by the user at his mobile is correct. Since the PIN is known only to the user, it provides two levels of authentication. Only if PIN and OTP are correct the user is allowed to proceed with the m-banking transaction that he initiated.

V.ANALYSIS OF THE PROPOSED IDEA

- Feistal networks used for encryption worksin a fashion called Format Preserving Encryption [9]. The plain text and the cipher text after encryption are in the same binary format.
- The encryption and decryption operations are very similar;a reversal of the key schedulewill suffice. Therefore the size of the code or circuitry required to implement such a cipher is minimal.
- This network uses EXOR logic operation that is invertible.
- Number of rounds increases security and hence difficult to break.
- 4-digit secret PIN plus ciphering provide additional two-tier security apart from password, the clientuses for the accessing his personal webpage of the bank site.PIN for flawless user identity and Ciphering toavoid man-in-the-browser attack during the session. Even if the user name and password are tracked using any of the techniques discussed, PIN (known only to the customer) provides additional security
- Entire SMS path from bank server to user mobile is made secure by encryption. The malware Trojan can still get the ciphered OTP but cannot decrypt it.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

VI. CONCLUSION

Nowadays we perform most of our bank transactions and m-commerce using smart phones and PDAs which comes handy. It saves lot of money and time and banking made lot easier. This has lots of comfort and convenience but exposes our m-banking transactions to new age risks like Phishing, MITB attack, identity theft etc. As sophistication and technology makes our lives lot more easier, Hackers also use the high-end technology to invent new means to acquire sensitive information such as usernames and passwords from bank or credit card customers. SMS-based OTP were introduced to prevent such threats which provides real-time authentication. The RBI has gone to the extent of making it mandate for all internet transactions. But even this is vulnerable to the threat of being hacked during the transmission of OTP from the bank server to the user mobile via the open mobile communication path. In this research paper we have proposed a novel method of combining secret 4-digit personal index number and feistal method of encryption for enhancing the security to the next level. This is a simple but an effective measure to combat the different online account thefts and frauds to secure our m-commerce transactions.

REFERENCES

1. Chang-Lung Tsai, Chun-Jung Chen." Trusted M-banking Verification Scheme based on a combination of OTP and Biometrics ", Journal of Convergence Vol 3,No. 3,23-30, 2012
2. K. Rieck, P. Stewin, and J.-P. Seifert ,"SMS-Based One-Time Passwords: Attacks and Defense" DIMVA 2013, LNCS 7967, Springer-Verlag Berlin Heidelberg 2013,pp. 150–159, 2013
3. Sri Rangarajan et al, "Securing SMS using Cryptography", International Journal of Computer Science and Information Technologies, Vol. 4 (2), 285 – 288, 2013
4. Chang-Lung Tsai, Chun-Jung Chen." Trusted M-banking Verification Scheme based on a combination of OTP and Biometrics ", Journal of Convergence Vol 3,No. 3,23-30, September 2012
5. Andrew Y. Lindell," Time versus Event Based One-Time Passwords", Aladdin Knowledge Systems, 2007
6. M. Viju Prakash, P. Alwin Infant and S. JeyaShobana, "Eliminating Vulnerable Attacks Using One-Time Password and PassText – Analytical Study of Blended Schema" Universal Journal of Computer Science and Engineering Technology 1 (2), 133-140, © 2010 UniCSE, ISSN: 2219-2158,Nov. 2010.
7. Dr.D.S. Rao et. al. ," One Time Password Security through Cryptography for Mobile Banking", International Journal of Computer Technologyand Applications, Sept-Oct 2011
8. DaudaSute, CISA."Man in the Browser – A Threat to Online Banking", ISACA Journal , Vol 4, 2013
9. S.Vidhya and K.Chitra, " Format Preserving Encryption using Feistel Cipher",Proceedings of International Conference on Research Trends in Computer Technologies ,2013
10. http://www.mspyapp.com.
11. D Sumathy et al,"A Framework of Security Issues and Standards for Efficient SMS", International Journal of Computer Technology & Applications,Vol 5 (2),469-478, ISSN:2229-6093,March-April 2014
12. http://en.wikipedia.org/wiki/Feistel_cipher.
13. http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html.
14. Ms. E.Kalaikavitha.,Mrs. Juliana Gnanaselvi," Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology",Research Inventy: International Journal Of Engineering And Science,Vol.2, Issue 10 ,Pp 14-17,ISSN(e): 2278-4721, ISSN,pp:2319-6483,April 2013