IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 8 (August. 2013), ||V3|| PP 25-33

Designing and Prototyping Encryptions Algorithms: Working As Secure M-Commerce Transaction of Broadcasting and Its Receiving Agent Based M-Commerce Model

Trivedi Jaydipkumar H, Darji Jitendrakumar H, Patel Hiteshkumar D, Trivedi Prakashkumar H

Assistant professor, Merchant College Of Management Studies And Research,Visnagar,Gujarat,India
Principal, Merchant Institute of Post Graduate Courses,Visnagar,Gujarat,India
Assistant professor, Merchant College Of Management Studies And Research,Visnagar,Gujarat,India
Assistant professor,GK&CK Bosmiya College, Jetpur,Gujarat,India

Abstract: - Broadcasting and Its receiving agent based M-commerce transaction done through automatic and semiautomatic way. At the initial stage (1) T.V Broadcasting, (2)Radio Broadcasting, (3) Telephone Broadcasting, (4) Web casting, (5) Satellite Broadcasting, (6) Cable Radio are Broadcasting recognizing as broadcasting agents. There are its receiving agents. Customer is establishing transaction on the basis of what the receiving agent provided. The work also proves and introduces E-mail services can be the advance payment system for the economical transaction. It clarifies the E-mail service that is emerging with the technology for payment system. At the embedded system of the architecture based on broadcasting and receiving agent based M-commerce Business Model, there is authentication and credit conformation performing. The work has highlighted encryption algorithm for secure M-commerce transaction. Designing and prototyping encryption algorithm regarded as a chief task of the work and prove its functionality as secure M-commerce transaction.

Keywords: - *M-Commerce*

I. INTRODUCTION

Broadcasting and Its receiving agent based M-commerce business model functioning in two different ways (1) Automatic and (ii) Semi Automatic way. Business transactions are also establishing in these two different ways. The work has highlighted embedded system at automatic way.[6] M-commerce background needs network based secure business transaction related to payment system. There are number of m-commerce payment transaction taken place like m-payment performed using sms.[1] Networking functionalities, Payment Cards, Payment intermediary have also been used as aspects for M-commerce based payment. The work has instructed encryption algorithm and perform designing and prototyping. There are certain challenges for existing algorithm of encryption for the secure transaction. The encryption algorithm needs to perform under m-commerce background. So existing algorithm need some reformations. The work has performed designing and prototyping encryption algorithm using username of the e-mail address of received e-mail for business transaction. Username of the e-mail address is taken as encryption key. The work has highlighted certain ways for obtaining e-mail base link of that customer who has performed business transaction and proved authorized customer. Customer has to submit there registration form before any transaction. The system has developed database for customer information. System also compare the database before any transaction.

II. LITERATURE REVIEW

"M-Payment between banks using sms" written by P Soni, he has written about payment system. SMS played important role for payment on M-commerce back ground. M-payment is an aspect that is establishing link between customer and merchant. "A new domain-based payment model" written by Diego Suarez, Joaquin Torres, Mildrey Carbonell and Jesus Tellez. They have written that there are three affecting factors. In the same work they indicated about payment card with networking functionality and about security solution. In his working, he instructed remote authentication protocol architecture for network smart card is described. The work also indicated Domain-based payment model. "A new approach towards encryption schemes: Byte-Rotation encryption algorithm has depicted by Sunita Bhati, Anita Bhati, S.K.Sharma. The work has proposed encryption algorithm "Byte-Rotation Encryption Algorithm" and "Parallel Encryption Model" for security. "Business model and transaction in mobile electronic commerce: requirements and properties" written by Aphrodite Tsalgatidou, Evaggelia Pitoura. The work instructed about business model and transaction. Data Encryption is explained in "An Introduction of Data base System written by C.J.Date, A. kannan, S. Swamynathan.

III. OBJECTIVES

The work has under mention objectives

- Study the encryption algorithms and considering the user name of the e-mail address as the secure encryption key.
- Designing and prototyping encryption algorithms
- Prove the advance strategy of encryption algorithms working as secure M-commerce transaction of broadcasting and its receiving agent based m-commerce model.

IV. RESEARCH METHODOLOGY

Research methodology is to be used in the present study is purely experimental.

V. HYPOTHESIS

1. Username of the e-mail address obtained through e-mail and username of the e-mail address working as secure encryption key.
2. E-mail service is working in payment system for broadcasting And its receiving agent based m-commerce model.
3. Encryption algorithm provide secure M-commerce transaction of broadcasting and its receiving agent based m-commerce model.

VI. ARCHTECTURE

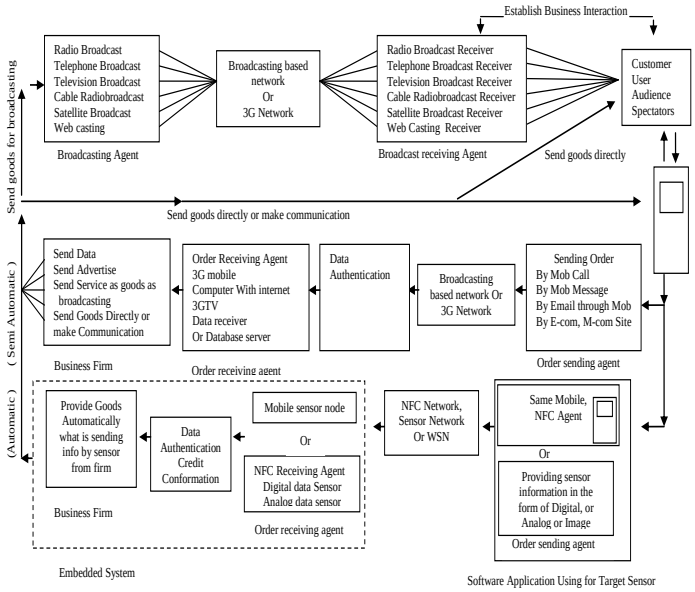


Figure 1 Architecture of the Broadcasting and its receiving agent based M-commerce business model

An architecture of the m-commerce model of broadcasting and its receiving agent based business model is instructing the ways of business transaction and system architecture.[6]

VII. ABOUT EXISTING ENCRIPTION ALGORITHMS

Data encryption: Any person will be using the system to access the database. Any stranger or unauthentic user who tries to bypass the system. The effective action against threat is data encryption. The data encryption is a technique for storing the data and transmitting sensitive data in encrypted state.

The unencrypted initial data is regarded as plaintext. The initial unencrypted data is encrypted by encryption algorithm. Using encryption keys (a kind of text on number) on a plain text and obtains the result as encrypted form is regarded as cipher text. Here the detail of the encryption is remaining public. Any one can read the encryption algorithm. But the encryption key is not made for public. It may be secret.

AS KINGFISHAR CATCH FIRE (Plain Text)

ELIOT (Encryption key)

Step 1 AS+KI NGFIS HERS+ CATCH FIRE

(Write the plain text into a state of length Equal to that of encryption key)

Step 2 "+" (Blank is indicating)

0119001109 1407060919 0805181900 0301200308 0006091805

(Convert the plain text by inter in the range 00-26 using blank = 00, A=01, B=02, J=10)

Step 3

0512091520 (use the step second for converting encryption key into integer form.

Step 4

0119001109 1407060919 0805181900 0301200308 0006091805

0512091520 0512091520 0512091520 0512091520 0512091520

(For all block convert character by the sum modulo 27 of its integer encoding and the integer encoding of character of the encryption key)

Step 5

FDIZB SSOXL MQ+GT HMBRA ERRFY

(Convert all integers encoding the result of step 4 by its character equivalent)

VIII. CHALLENGES

(1) Will the exiting algorithm of encryption work at network based M-commerce background for secure transaction?
(2) How can encryption algorithm link with the authorized user or customer on M-commerce background?
(3) What about the simplicity of the algorithm?
(4) What about complicated mathematical computation of the algorithm?

IX. NEED FOR POROTOTYPING AND DESIGNING

(i) The existing algorithm of encryption is using encryption key like "ELIOT" is not providing any authentic information of a genuine customer or so it need authentic encryption key which provide some fact about customer authenticity and senders information. System failed to get authorization of a customer.

Where as, propose prototype encryption algorithm using user name of e-mail address as an encryption key. The user name of e-mail address based encryption key is indicating the sender's information of the e-mail transaction on m-commerce back ground. At the end, system obtained senders authentication for the further transaction. Example mrjlecturer@yahoo.com

(ii) The existing algorithm has complicated mathematical problem like sum modulo and indication of remainder etc. for encryption of the text. Where as the propose technique provide only simple sum and subtraction and conversion related to alphabetical state of the plain text.

(iii) M-commerce transaction needs secure transaction so it needs some advance encryption algorithm.

X. DESING ENCRIPTION ALGORITHM

Background of the algorithm indicates that the user name of e-mail address using as encryption key. The user name is unique for the system on a network while it is using user name of e-mail address as encryption key. User can perform M-commerce transaction from any where of the world. System needs authorization of the customer and allow them to perform M-commerce transaction. So the study can indicates user name of e-mail address as encryption key.

Step 1:

TRIVEDI-JAYDIPKUMAR-H

(Plain text as message obtained)
(Converts the character to its related alphabetical digit like A=01, B=02, C=03, D=04 …..)
(In the plain text blanks seems as "-")
(Indicates Space as 00)

Step 2:

20180922050409001001 25040916112113011800 08

(Decide the digital block of the string as per the length of user name of e-mail address's digit)

Step 3:

mrjlecturer (obtained from mrjlecturer@yahoo.com)

(The encryption key formed on the basis of user name of e-mail address taken form e-mail message for business Transaction is taking user name of e-mail address Only without "@" and rest of the address like yahoo mail.com)

131810120503202118051 8 (Encryption key got from username)

(Converts the character to its related alphabetical Digit like A=01, B=02, C=03, D=04 …..)

Step 4:
20180922050409001001250409161121130118000813181012050320211805133181012050320211805 3336193410072921280643 17272623261621391813
(Sum the digital block of the string with Encryption key)

Step 5:
CCCFAICDA00GBIBABH0FDC AGBGBFBCBFAFBACIAHAC
(The obtained result of the sum from step 4 converted the digital string into alphabetical String like 3=C, 9=I, and keep Zero "0" remain Same for further task, It means "0" is encrypted as "0" only.)

Encrypted Message:
CCCFAICDA00GBIBABH0FDC AGBGBFBCBFAFBACIAHAC

Step 6:
CCCFAICDA00GBIBABH0FDC AGBGBFBCBFAFBACIAHAC
3336193410072921280643 1727262 3261621391 813
(Converted the alphabetical string into digital String like C=3, I=9, and keep Zero "0" remain Same for further task, It means "0" is encrypted as "0" only.)

Step 7:
3336193410072921280643 17272623261621391813
13181012050320211805 13181012050320211805
20180922050409001001250409161121130118000813181012050320211805 3336193410072921280643
(Subtracted the digital block of the string with Encryption key)

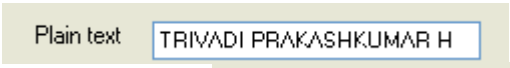
Step 8:
20180922050409001001250409161121130118000813181012050320211805 3336193410072921280643
T R I V E D I - J A Y D I P K U M A R - H
(Obtained alphabetical string on the basis of result acquired from subtraction)

CODES AND SIMULATOR

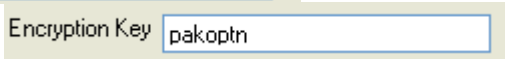
Simulator:

INPUT DATA

1. Plain Text:

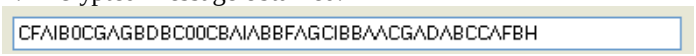


2. Encryption Key:



OUTPUT DATA

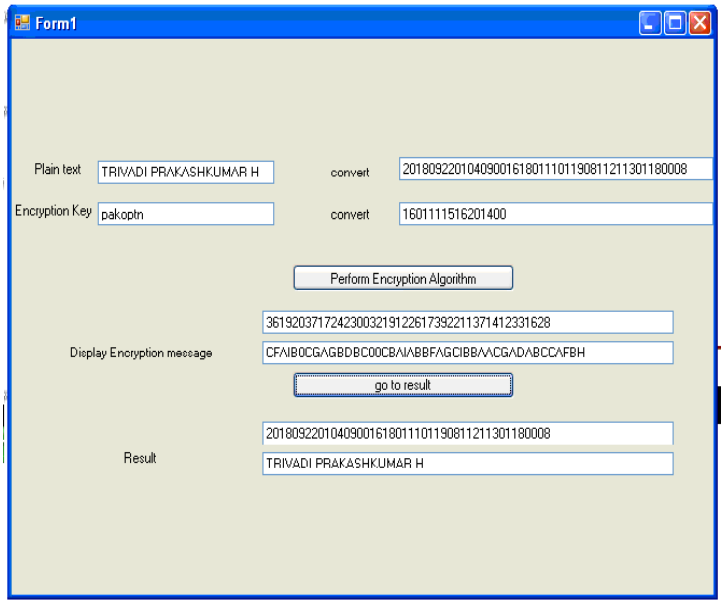
1. Encrypted Message obtained:



2. Ultimate Result:

5. User name and other information indicated from received e-mail at system level

Delivered-To: profjaydip@gmail.com
Received: by 10.64.229.75 with SMTP
id so11csp327556iec; Fri, 2 Aug 2013 03:58:57 -0700 (PDT)
X-Received: by 10.66.190.198 with SMTP id gs6mr9634614pac.49.1375441137530;
Fri, 02 Aug 2013 03:58:57 -0700 (PDT)
Return-Path: <pakoptn@rediffmail.com>
Received: from rediffmail.com (f5mail-224-167.rediffmail.com. [114.31.224.167])
by mx.google.com with SMTP id ql10si6480334pbb.160.2013.08.02.03.58.55
for <profjaydip@gmail.com>;
Fri, 02 Aug 2013 03:58:57 -0700 (PDT)



Codes:

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Text;
using System.Windows.Forms;
namespace encryption
{public partial class Form1 : Form
   {public Form1()
    {InitializeComponent();}
private void txtplaintext_Leave(object sender, EventArgs e)
{int asccode, i;
char[] c = new char[txtplaintext.Text.Length];
string str = "";
c = txtplaintext.Text.ToCharArray();
for (i = 0; i < txtplaintext.Text.Length; i++)
{asccode = (int)c[i];
if (asccode >= 65 && asccode <= 90)
{asccode = asccode - 64;
if (asccode <= 9)
str = str + "0" + asccode;
else
str = str + asccode;}
if (asccode >= 97 && asccode <= 122)
{ asccode = asccode - 96;
if (asccode <= 9)
str = str + "0" + asccode;
else
str = str + asccode;}
if (asccode == 32)
str = str + "00";     }
txtconplain.Text = str; }
private void textBox1_TextChanged(object sender, EventArgs e)
{        }
private void button1_Click(object sender, EventArgs e)
{int len1 = txtconplain.Text.Length;
 int len2 = txtconenckey.Text.Length;
```

```
 int i, V;
 decimal value1, value2, total;
 string s1 = "", s2 = "", S = "";
 txtsum.Text = "";
 for (i = 0; i < len1; i = i + len2)
{if ((txtconplain.Text.Length - i) < len2)
{s1 = txtconplain.Text.Substring(i, txtconplain.Text.Length - i);
s2 = txtconenckey.Text.Substring(0, txtconplain.Text.Length - i);
}else
{s1 = txtconplain.Text.Substring(i, len2);
s2 = txtconenckey.Text.Substring(0, s1.Length);}
value1 = decimal.Parse(s1);
value2 = decimal.Parse(s2);
total = value1 + value2;
if (total.ToString().Length == s1.Length)
txtsum.Text = txtsum.Text + total.ToString();
else
txtsum.Text = txtsum.Text + "0" + total.ToString();
}char[] c = new char[txtsum.Text.Length];
c = txtsum.Text.ToCharArray();
for (i = 0; i < txtsum.Text.Length; i++)
{V = int.Parse(c[i].ToString());
c[i] = Convert.ToChar(64 + V);
if (c[i] == '@')
S = S + "0";
else
S = S + c[i];}
txtsummessage.Text = S;}
private void textBox2_TextChanged(object sender, EventArgs e)
{  }
private void txtencrykey_Leave(object sender, EventArgs e)
{if(txtencrykey.Text.Length ==7)
txtencrykey.Text = txtencrykey.Text + " ";
int asccode, i;
char[] c = new char[txtencrykey.Text.Length];
string str = "";
c = txtencrykey.Text.ToCharArray();
for (i = 0; i < txtencrykey.Text.Length; i++)
{asccode = (int)c[i];
if (asccode >= 65 && asccode <= 90)
{asccode = asccode - 64;
if (asccode <= 9)
str = str + "0" + asccode;
else
str = str + asccode;}
if (asccode >= 97 && asccode <= 122)
{asccode = asccode - 96;
if (asccode <= 9)
str = str + "0" + asccode;
else
str = str + asccode;}
if (asccode == 32)
str = str + "00"; }
txtconenckey.Text = str;}
private void textBox3_TextChanged(object sender, EventArgs e)
{  }
private void button2_Click(object sender, EventArgs e)
{int len1 = txtsum.Text.Length;
int len2 = txtconenckey.Text.Length;
```

```
int i, V=0;
decimal value1, value2, total;
string s1 = "", s2 = "", S = "";
txtsub.Text = "";
for (i = 0; i < len1; i = i + len2)
{if ((txtsum.Text.Length - i) < len2)
{s1 = txtsum.Text.Substring(i, txtsum.Text.Length - i);
s2 = txtconenckey.Text.Substring(0, txtsum.Text.Length - i);
}else{s1 = txtsum.Text.Substring(i, len2);
s2 = txtconenckey.Text.Substring(0, s1.Length);}
value1 = decimal.Parse(s1);
value2 = decimal.Parse(s2);
total = value1 - value2;
if (total.ToString().Length == s1.Length)
txtsub.Text = txtsub.Text + total.ToString();
else
txtsub.Text = txtsub.Text + "0" + total.ToString();
}char[] c = new char[txtsub.Text.Length];
c = txtsub.Text.ToCharArray();
for (i = 0; i < txtsub.Text.Length; i = i + 2)
{V = int.Parse(txtsub.Text.Substring(i, 2));
c[i] = Convert.ToChar(64 + V);
if (c[i] == '@')
S = S + " ";
else
S = S + c[i];
}txtorimsg.Text = S; } } }
```

XI. PROVES THE TRANSECTION AS SECURE M-COMMERCE TRANSECTION OF BROADCASTING AND ITS RECEIVING AGENT BASED M-COMMERCE MODEL

What the system obtained from e-mail sender side's information is important for embedded system. The system need to recognize the customer on a network or on m-commerce background. And the user name of e-mail address provides some link and information of the e-mal sender.

PARAMETERIZED DATA IN ENCRYPTION ALGORITHM:

1. Data in 1st Cycle parameterized in algorithm:

1. Plain text as message to be parameterized in algorithm:
   TRIVEDI-JAYDIPKUMAR-H
2. Encryption Key used by algorithm:
   mrjlecturer
3. Obtained Encrypted Message parameterized by algorithm:

   CCCFAICDA00GBIBABH0FDC AGBGBFBCBFAFBACIAHAC

4. Ultimate Result Obtained Through Algorithm:
   TRIVEDI-JAYDIPKUMAR-H

2. Data in 2nd Cycle parameterized in algorithm:

1 Plain text as message to be parameterized in algorithm:
   DARJI-JITENDRAKUMAR
2 Encryption Key used by algorithm:
   mcajayesh@yahoo.com
3 Obtained Encrypted Message parameterized by algorithm:
   AG0DAIB0A0BEAEBHBH AHAG0EBH0BCFBFCB0ICA
4 Ultimate Result Obtained Through Algorithm:
   DARJI-JITENDRAKUMAR

System Obtains Business Transaction's E-Mails and Its Detail for More Customer Authorization Purposes:

1. Data in 1st Cycle that is obtained show original from system e-mail inbox at profjaydip@gmail.com

FIRST CYCLE RELATED E-MAILS

1. System E-Mail address: profjaydip@gmail.com
2. Customer E-Mail address: mrjlecturer@yahoo.com

Detail of system e-mail which obtained from customers mail: At the G-mail go to show original obtained below mention information of email sender customer.

Delivered-To: profjaydip@gmail.com
Received: by 10.64.229.75 with SMTP id so11csp94386iec;
Mon, 22 Jul 2013 21:44:06 -0700 (PDT)
X-Received: by 10.49.13.229 with SMTP id k5mr36234047qec.64.1374554645798;
Mon, 22 Jul 2013 21:44:05 -0700 (PDT)Return-Path: <mrjlecturer@yahoo.com>
Received: from nm42-vm3.bullet.mail.bf1.yahoo.com (nm42-vm3.bullet.mail.bf1.yahoo.com.
[216.109.114.190])by mx.google.com with ESMTPS id 16si11956435qeb.145.2013.07.22
.21.44.05 for <profjaydip@gmail.com>(version=TLSv1 cipher=RC4-SHA bits=128/128);Mon, 22 Jul 2013
21:44:05 -0700 (PDT) (Continue)

SECOND CYCLE RELATED E-MAILS

1. System E-Mail address: profjaydip@gmail.com
2. Customer E-Mail address: mcajayesh@yahoo.com

Detail of system e-mail which obtained from customers mail: At the G-mail go to show original obtained below mention information of email sender customer.

Delivered-To: profjaydip@gmail.com
Received: by 10.64.229.75 with SMTP id
so11csp264956iec;
Thu, 1 Aug 2013 02:22:03 -0700 (PDT)
X-Received: by 10.67.10.236 with SMTP id ed12mr2801616pad.153.1375348922903;
Thu, 01 Aug 2013 02:22:02 -0700 (PDT)
Return-Path: <mcajayesh@yahoo.co.in>
Received: from nm18-vm8.bullet.mail.sg3.
yahoo.com(nm18-vm8.bullet.mail.sg3.yahoo.com. [106.10.149.103])by mx.google.com with SMTP id
x6si1878358pab.49.2013.08.01.02.22.01
for <profjaydip@gmail.com>;Thu, 01 Aug 2013 02:22:02 -0700 (PDT) (Continue)

XII. ANALYSIS OF THE DATA

There are two cycle's results of the proposed algorithm.

Input Data Result:

At First Cycle:

1. Plain Text: TRIVEDI-JAYDIPKUMAR-H
2. Encryption Key: mrjlecturer
3. Encrypted Message obtained:
   CCCFAICDA00GBIBABH0FDC AGBGBFBCBFAFBACIAHAC
4. Ultimate Result: TRIVEDI-JAYDIPKUMAR-H
5. User name and other information indicated from received e-mail at system level:
   Delivered-To: profjaydip@gmail.com

Received: by 10.64.229.75 with SMTP id so11csp94386iec;
Mon, 22 Jul 2013 21:44:06 -0700 (PDT)
X-Received: by 10.49.13.229 with SMTP id k5mr36234047qec.64.1374554645798;
Mon, 22 Jul 2013 21:44:05 -0700 (PDT)
Return-Path: <mrjlecturer@yahoo.com>
Received: from nm42-vm3.bullet.mail.bf1.yahoo.com (nm42-vm3.bullet.mail.bf1.yahoo.com.
[216.109.114.190])etc. (Continue)

At Second Cycle:

1. Plain Text: DARJI-JITENDRAKUMAR
2. Encryption Key: mcajayesh
3. Encrypted Message obtained:
   AG0DAIB0A0BEAEBHBH AHAG0EBH0BCFBFCB0ICA
4. Ultimate Result: DARJI-JITENDRAKUMAR

5. User name and other information indicated from received e-mail at system level:

Delivered-To: profjaydip@gmail.com
Received: by 10.64.229.75 with SMTP id so11csp264956iec;
Thu, 1 Aug 2013 02:22:03 -0700 (PDT)
X-Received: by 10.67.10.236 with SMTP id ed12mr2801616pad.153.1375348922903;
Thu, 01 Aug 2013 02:22:02 -0700 (PDT)
Return-Path: mcajayesh@yahoo.co.in
Received: from nm18-vm8.bullet.mail.sg3.
yahoo.com (nm18-vm8.bullet.mail.sg3.yahoo.com. [106.10.149.103])

1. Data can be encrypted using proposed algorithm on network based unique identification encryption key.
2. The open messages which are in encrypted form, so none can understand and it will remain secret.
3. Received E-mail from customer's side has some identification at show original option in inbox.

XIII. CONCLUSION

The analysis implies that plaintext have encrypted and obtained as secret message. Thus m-commerce transactions have derived from security level. Broadcasting and its receiving agent based m-commerce model has embedded system for performing transactions which included encryption algorithm as security level.

REFERENCES

[1] P Soni, M-Payment between banks using sms, IEEE 2010,Vol 98, No.6, 2010.
[2] S Diego, T Joaquin, C Mildery, T Jesus, A new domain- based payment model for emerging mobile commerce scenarios, IEEE 2007.
[3] S Bhati, A Bhati, S Sharma, A new approach Towards encryption schemes: Byte-Rotation Encryption Algorithm, World Congress on engineering and computer science 2012 vol II, San Fransisco,USA.ISSN: 2078-0958.
[4] T Aphrodite, P Evaggelia, Business Models and Transactions in mobile electronic commerce: Requirements and Properties, Elsevier, Computer Networks 37(2001)
[5] C.J Date, A Kannan, Swamynathan, An Introduction to Data base Systems, Eightth Edition, Chap.17 P.433.
[6] J.H.Trivedi,Dr J G Padya, P H Trivedi, Dr A N Jani, Broadcasting and Its receiving Agent Based M-Commerce Business Model, Presented as poster presentation in cross disciplinary international seminar held at H.N.G.University, Patan.India. And gone for Publishing in the University Journal.