Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 3, March 2017, pg.50 – 57

INFORMATION SECURITY USING BLOWFISH ALGORITHM IN E-BANKING

Anupam Baruah[1], Prof.(Dr.)Lakshmi Prasad Saikia[2]

[1]Research Scholar, Dept. of Computer Science & Engineering, Assam down town University, India

[2]Professor, Dept. of Computer Science & Engineering, Assam down town University, India

[1] anupambaruah04@gmail.com; [2] lp_saikia@yahoo.co.in

Abstract— E-Banking provides all banking services to its users over the internet. Some of the services include paying of bills, Fund transfer, transfer, viewing account statement, etc. Users can easily access their e-banking account through internet via computers and Smartphone using wi-fi or 3g/4g connection. But security of fund transaction is a very big issue. There is a possibility to hack user's account information by hackers at any time over internet. Cryptography is a best technique for encrypt data from outside Hackers. In this paper we implement a banking system by using Blowfish algorithm. This system will provide a secure web base application where only authorize users can access all information using a valid secret key.

Keywords— Cryptography, Symmetric key encryption, Asymmetric key encryption, Blowfish algorithm

I. INTRODUCTION

In modern era, Internet Banking plays an important roll of our daily life. E-banking means services provided by the banks over internet. Some services include fund transfer, bill payment, and view account statement online. Users can do all services at any time because there is no global time for internet. But we should keep our important information from hackers. So data encryption is an important part in this system. Cryptography provides the necessary tools for accomplishing secure and authenticated transactions[1]. There are many cryptographic algorithms like RSA encryption algorithm, DSA encryption algorithm, Blowfish algorithm, two fish algorithm, AES algorithm etc. In the system implementation we are using Blowfish algorithm as encryption techniques which is a symmetric key block cipher design.

MEANING OF CRYPTOGRAPHY:

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. It deals with the actual securing of digital data. The primary objective of using cryptography is to provide the four fundamental services i.e.

a) *Confidentiality*: It is a security service that keeps the information from an unauthorized person. It is also referred to as privacy or secrecy.
b) *Data integrity*: It deals with the identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently.
c) *Authentication*: It provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.
d) *Non-repudiation*: It is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

SYMMETRIC KEY ENCRYPTION

The encryption process where same keys are used for encrypting and decrypting the information is known as symmetric key encryption. The study of symmetric cryptosystem is referred to as symmetric key cryptography.

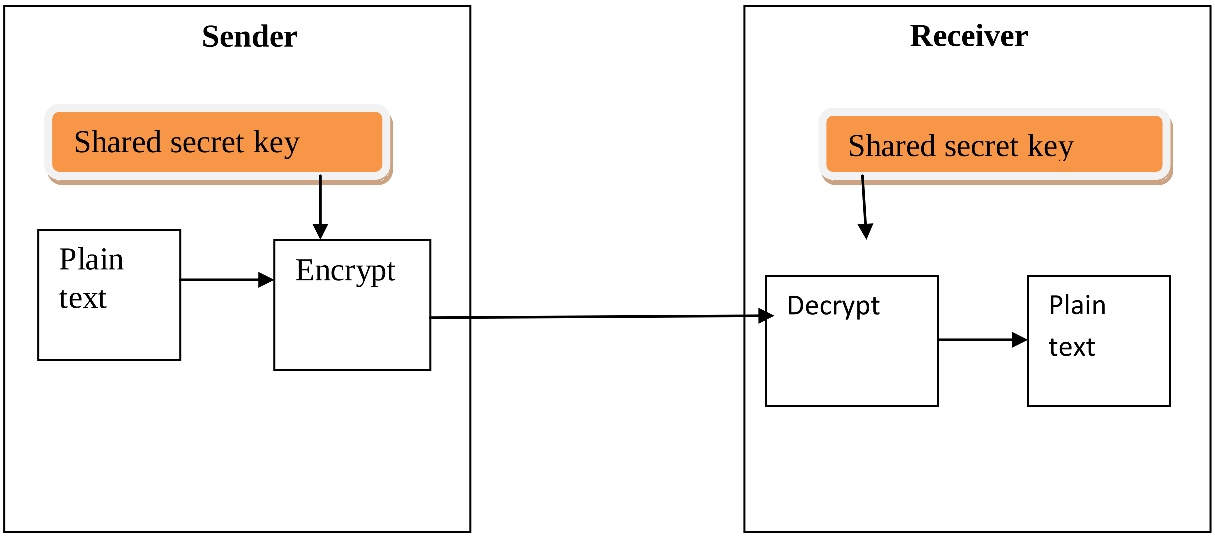


Fig 1.1

ASYMMETRIC KEY ENCRYPTION

In asymmetric key encryption different keys are used for encrypting and decrypting the information. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting cipher text is feasible.

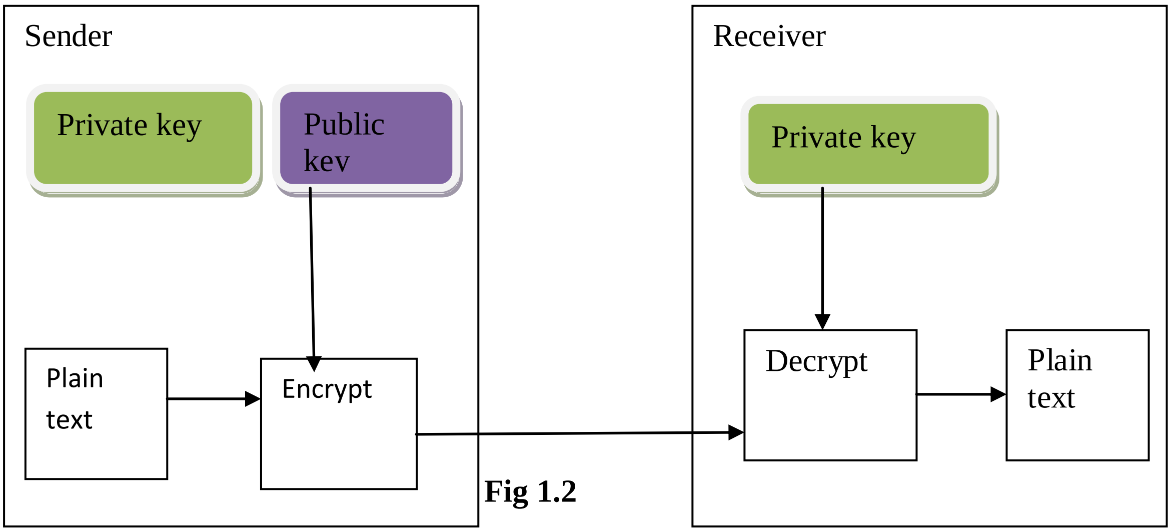


Fig 1.2

Blowfish

In 1993, Bruce Schneier designed Blowfish algorithm. The elementary operators of Blowfish algorithm include table lookup , addition and XOR. Blowfish is a 64bit block cipher and can encrypt data on 32-bit microprocessors. It can also run in less than 5k of memory. It uses addition, XOR, lookup table with 32-bit operand [2]. The algorithm consists of two parts: a key-expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several subkey arrays totalling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words.

II. Related Work

In 2010, Diaa Salama Abd Elminaam, Hatem Mohamed Abdul Kader and Mohiy Mohamed Hadhoud evaluated the performance of Symmetric Encryption Algorithms. They used some selected algorithms which are AES, DES, 3DES, RCC, BLOWFISH in their model [1].

In 2013, Tanjyot Aurora and Parul Arora implemented a secret key block cipher algorithm "Blowfish algorithm" from the prospective cryptology. They made a design and implementation of Blowfish algorithm by which client can manage their userid and password efficiently. An Implementation of Feistel network for encryption files is also examined in their work [2].

In 2014, Mrs Veena Jose and Ms. C. Divya implemented Blowfish algorithm for secure data transmission. The data to be transmitted is stored in a file and the file is encrypted using Blowfish algorithm. This encrypted file is communicated among the group members, such that they can easily decrypt the file using same key which is known to them [3].

In 2014, Ms Neha Khatri and Prof. V. K Kshirsagar introduced an algorithm works on the same line as DES and it consumes block coding with blocks of a size of 64 bit. Blowfish became quite popular after its advent. The proposed algorithm of the Blowfish can achieve efficient data encryption up to 4 bits per clock [4].

In 2015, Saikumar manku and K vasanth introduced an algorithm for information security is designed and analysed. The work is done for networking and communication applications for enhanced network security and defence applications. They presented simulation result that shows encryption and decryption process using Blowfish algorithm [5].

III.Methodology

A. Customer registration process:

In my system both admin and stuff can add customer .After inserting all details of customer an account number and a secrete key will generate against each customer. Every customer must remember his/her secrete key. At the time of registration all customer's data are converted to cipher text by blowfish algorithm with a key. Same key must be use to decrypt the cipher text to plain text.

Encryption process:

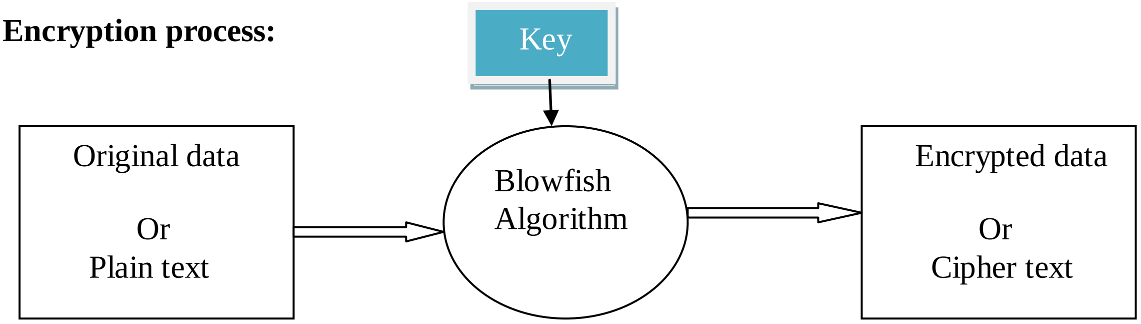


Fig 3.1

In this encryption process, some data like account number, phone number, secrete key, date of birth etc of each customer are encrypted by blowfish algorithm with a encryption key.

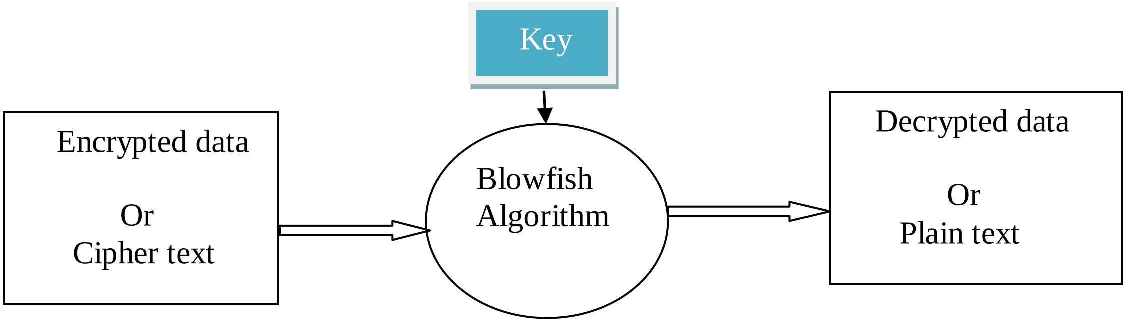


Fig 3.2

After successful login customer have to insert secret key to decrypt all encrypted text. Here the same key uses to decrypt the text.

The basic algorithm for Blowfish algorithm is illustrated as follows.

```
Divide x into two 32-bit halves: xL, xR
    For i = 1to 16:
          xL = XL XOR Pi
          xR = F(XL) XOR xR
          Swap XL and xR
          Swap XL and xR (Undo the last swap.)
          xR = xR XOR P17
    xL = xL XOR P18
    Recombine xL and xR
Output 64 bit X(Cipher text).
```

IV. SIMULATION AND RESULT

In this paper, we have simulated Encryption and decryption part in PHP language. There are mainly three (3) sections like admin section, stuff and customer. Admin can do all operations including creation of customer and stuff, updating of customer and stuff details, deletion of stuff and customer details etc. Stuff only can create customer and also can update customer's details. Customers can view their account details, can transfer fund, can add beneficiary details, etc.

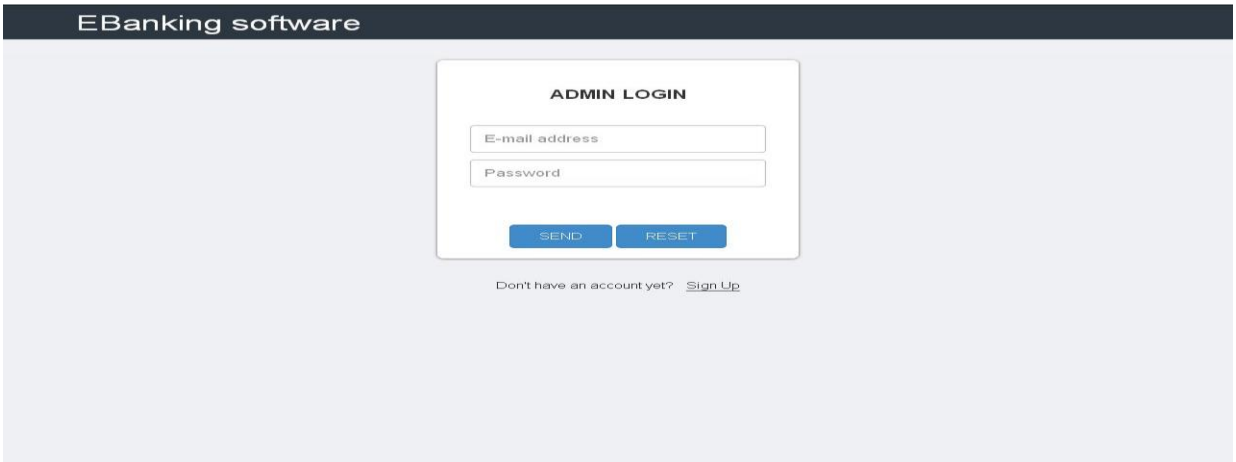
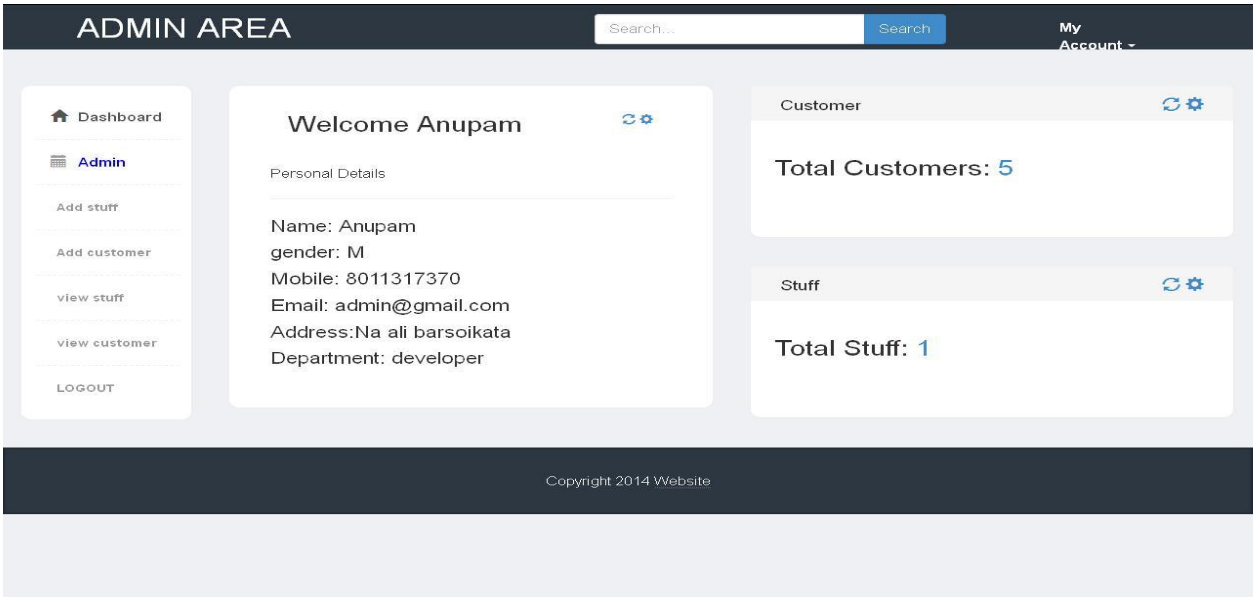


Fig 4.1: Admin login area

Admin can login using emailed and password. After successful login page redirects to admin dashboard.



Welcome Anupam

Personal Details

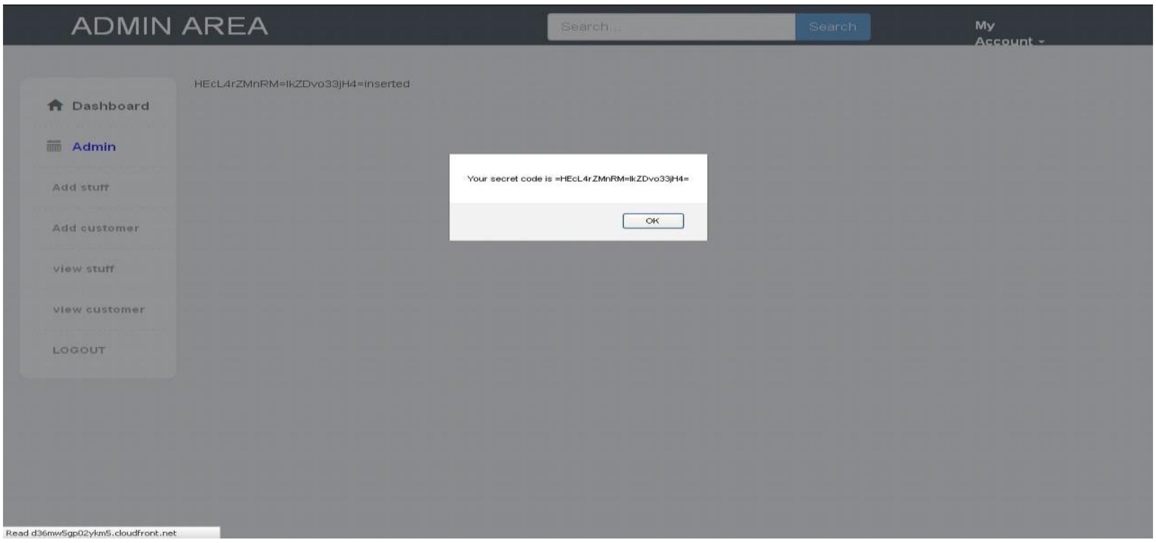
Name: Anupam
gender: M
Mobile: 8011317370
Email: admin@gmail.com
Address:Na ali barsoikata
Department: developer

Total Customers: 5

Total Stuff: 1

Fig 4.2: Admin Dashboard

Admin can view, edit, and delete stuff/customers. There is a change password link where admin can update his/her password.

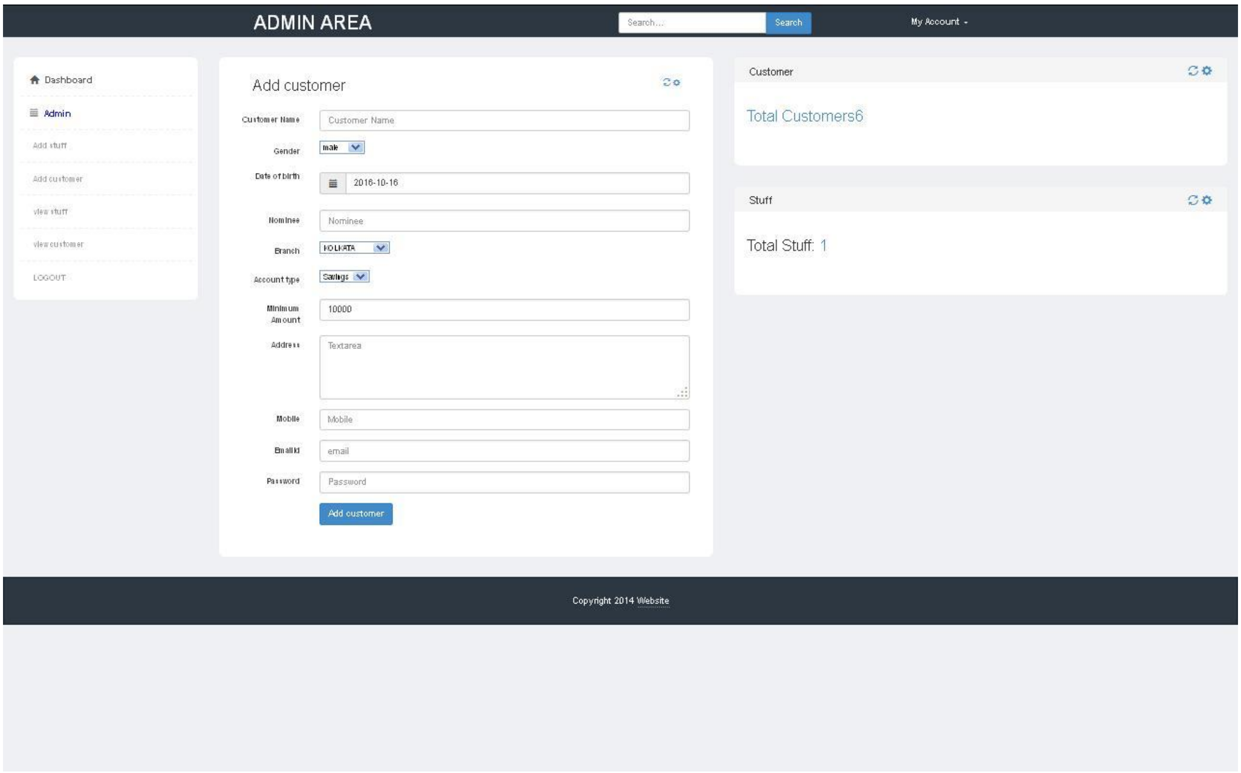


HEcL4rZMnRM=IkZDvo33jH4=inserted

Your secret code is =HEcL4rZMnRM=IkZDvo33jH4=

Read d36mw5gp02ykm5.cloudfront.net

Fig 4.3: Generate secret key



Add customer

Customer Name: Customer Name
Gender: male
Date of birth: 2016-10-16
Nominee: Nominee
Branch: KOLKATA
Account type: Savings
Minimum Amount: 10000
Address: Textarea
Mobile: Mobile
Email id: email
Password: Password

Customer

Total Customers6

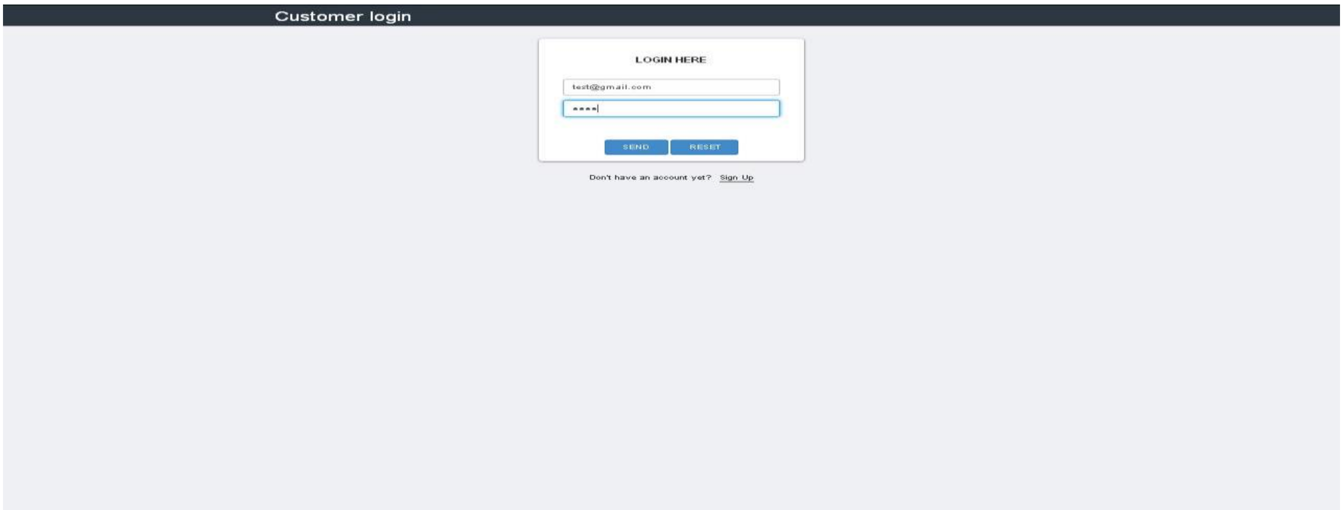
Stuff

Total Stuff: 1

Copyright 2014 Website

Fig 4.4: Customer registration

In customer registration form, admin can add customers to the system. He can edit or delete customers also.


Customer login

LOGIN HERE

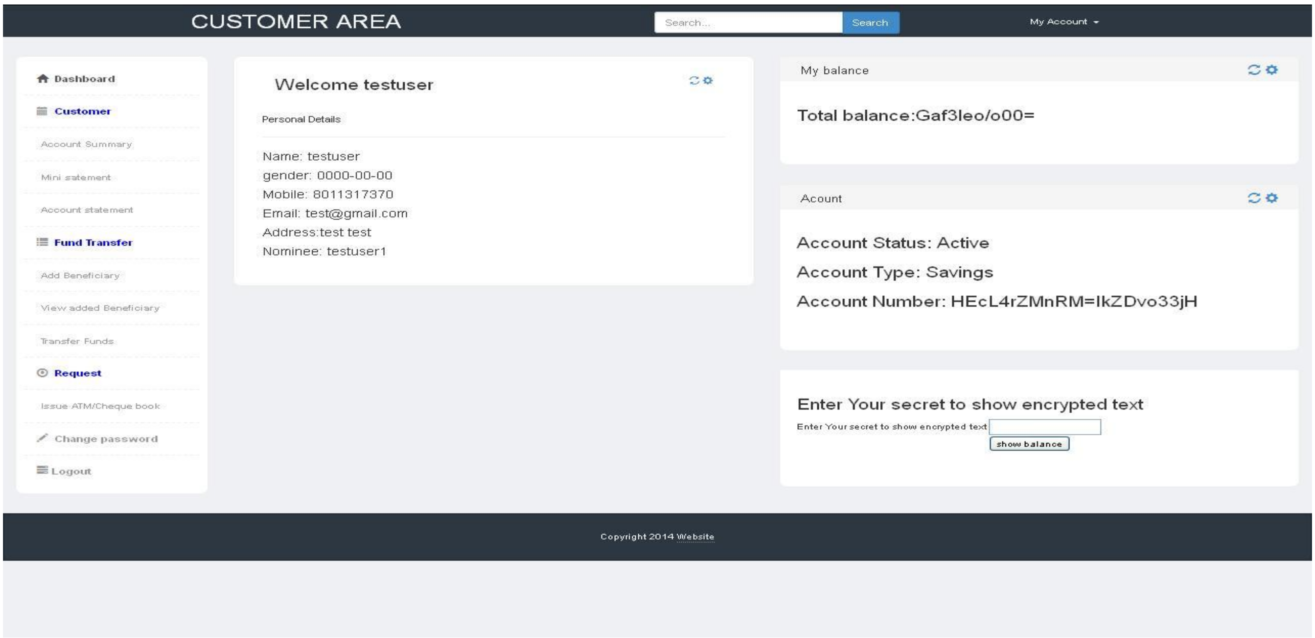
test@gmail.com

••••

Don't have an account yet? Sign Up

Fig 4.5: Customer login area

Customer can login to the system using customer user-id and password .After successful login page redirect to customer dashboard page where customers can view their profile, can add beneficiary, can transfer funds etc.


CUSTOMER AREA

Welcome testuser

Personal Details

Name: testuser
gender: 0000-00-00
Mobile: 8011317370
Email: test@gmail.com
Address:test test
Nominee: testuser1

My balance

Total balance:Gaf3leo/o00=

Acount

Account Status: Active

Account Type: Savings

Account Number: HEcL4rZMnRM=IkZDvo33jH

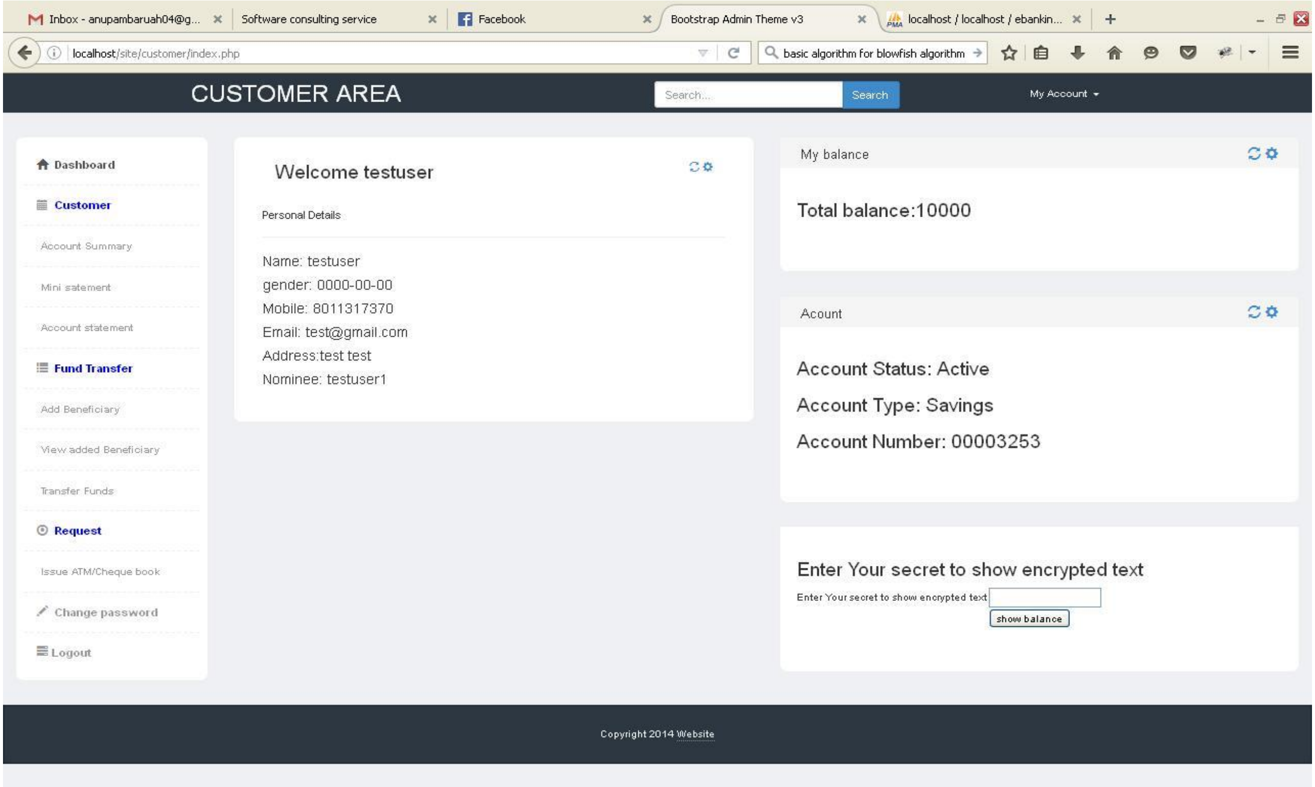
Enter Your secret to show encrypted text

Enter Your secret to show encrypted text

Copyright 2014 Website

Fig 4.6: Customer dashboard with encrypted balance and account number

In customer dashboard area account number and total balance is encrypted using blowfish algorithm. Customers must enter secret key to decrypt the cipher text.



Welcome testuser

Personal Details

Name: testuser
gender: 0000-00-00
Mobile: 8011317370
Email: test@gmail.com
Address:test test
Nominee: testuser1

My balance

Total balance:10000

Acount

Account Status: Active
Account Type: Savings
Account Number: 00003253

Enter Your secret to show encrypted text

Enter Your secret to show encrypted text

show balance

Fig 4.7: Customer dashboard with decrypted balance and account number

Total balance and account number is converted to human readable plain text after putting the secret key to the input field.

V. Conclusion

In modern communication system, Information security plays an important role. All confidential or important information send on internet, so it is very important to keep records secure. So to protect our information, we should take importance in Privacy, integrity, confidentiality and non repudiation. When customer transfers money to any beneficiary over internet the protection of data against security threats is a major issue. During transaction the data must be protected from unauthorized access. In our system, we have used blowfish algorithm. The algorithm encrypts information to unreadable format and then sends over internet which increases the level of security dimensions.

References

[1] Diaa Salama Abd Elminaam, Hatem Mohamed Abdul Kader and Mohiy Mohamed Hadhoud, “evaluated the performance of Symmetric Encryption Algorithms”, International Journal of Network security, Vol 10, No.3,PP 2013-219,May 2010.

[2] Tonjyot Aurora and Parul Arora, ”Blowfish Algorithm”, International Journal of Computer Science and Communication Engineering(IJCSCE)”, ISSN 2319-7080,June 2013,pp 238-243.

[3] Mrs Veena Jose and Ms C Divya, ”Secure multicasting using Blowfish algorithm”, IJAICT, Volume 1,ISSUE 4,August 2014,ISSN 2348-9928, PP 411-414.

[4] Ms NehaKhatri – Valmik1, Prof. V. K Kshirsagar, “Blowfish Algorithm”, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, e-ISSN: 2278-0661, p- ISSN: 2278-8727, PP 80-83.

[5] Saikumar Manku and K Vasanth, “Blowfish encryption algorithm for information security”, ARPN Journal of engineering and applied Sciences, Vol 10,No.10,June 2015,ISSN 1819-6608,PP 4717-4719.