Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.776828

IMPLEMENTATION OF E-BANKING TRANSACTION SYSTEM USING ELGAMAL DS

Ajit Kumar Singh[1], Moumita Kumar Roy[2], Sunil Karforma[3], Sripati Mukhopadhyay[4]

[1]Department of Computer Science, Netaji Mahavidyalata , Arambagh , Hooghly,India
[2]Department of Electronics, Netaji Mahavidyalata , Arambagh , Hooghly,India
[3] Department of Computer Science, The University of Burdwan, Purba Burdwan, India
[4] Ex-Professor, Department of Computer Science, The University of Burdwan, Purba Burdwan, India

Abstract: *In today's world we are being accommodated in a digital era, we are now able to do most of the job in virtual digital online platform. In present time we have almost forgot to visit bank physically. Now we are being accustomed with online banking system, which is accessible 24X 7 and from wherever we are. This virtual form of Banking is very beneficial for the customers for its enormous utility and use ability. The major challenge associated with online banking is the security. The accounts of the customers should be highly secured by some technology so that the customers would not face any kind of fraudulent transaction while using online banking. Digital signature is a way of securing bank accounts just the way we need to sign physical documents in bank while making any transaction, to authenticate the validity of the customer. There is several technologies for encryption of digital signature but Elgamal method is one of the most popular public key cryptography technology. In this paper the method of implementation of digital signature is discussed following which Elgamal DS can be employed with the help of proper code.*

Keywords: *E-Banking, Digital Signature, cryptography, Elgamal, Security*

I. Introduction

Electronic Banking or E-Banking or Online Banking is an easy way to efficiently access our bank account from everywhere and any time with the help of internet and mobile or laptop or desktop etc. E-Banking offers almost all the services of their customer for which they need to visit bank branches and need to wait in long queues to retrieve bank services. Not only the customer, bank itself is also benefited with E-Banking by reducing transaction cost, staff remuneration and branch offices. But the major expected feature of E-Banking is security and privacy because we are transferring our hard earning money in virtual form. So online transaction need utmost care to avoid fraudulent transaction.

Cryptography is a tool used for protecting digital data. Basically, cryptography encrypt the ordinary text and only authenticate recipient decrypt it. There are many ways to encrypt and decrypt the text like password, biometric, steganography, digital signature etc. Digital signature is a digital code attached with digital document that transmitted through internet for verifying

content and secure identity. Our main focus is implementing E-Banking Transaction System using Elgamal DS.

Signature is used to authenticate and give confirmation of original document. Digital signature is a mechanism for authenticating an electronic document or message by using encryption techniques. The entire process of Digital Signature has two participant (signer and verifier) and three phases (key generation, signing and verification). Signer uses his private key to sign document and sends to the verifier uses signer's public key to verify the signature. ElGamal is a Digital signature scheme. It is described by Taher ElGamal in 1984. ElGamal is faster than RSA. It has been implemented several situations like encryption, cloud and even different combinations of other algorithms to improve them. The ElGamal algorithm provides some benefits within cryptography.

II. Literature Review

Digital signature has become an inevitable part of our everyday life in modern days the most important part digital signature is its security. There are many algorithms related to digital signature cryptography, but ElGamal method is a popular asymmetric public key Cryptography method in present time. While considering the level of security it is one of the most secure used for digital signature. Another popular public key cryptography is RSA algorithm which was proposed in 1976 by Ron Rivest, Adi Shamir, and Leonard Adleman. MIT(Massachusetts Institute of Technology) , based on prime factors method [7] suggest public key cryptography algorithm which combines ElGamal and RSA both the algorithms.

Laryoshyna [2] has started the security standards of digital signature using ElGamal algorithm against brute force attack and found that it is not the one with highest security. Based on their experiment they have recommended that ElGamal algorithm should use high primitive numbers and the primitive routes should not be chosen within the first five integers to delay brute force attack this factor may increase the security of the digital signature.

Haraty et. al.[3] have made a comparative study between the classical ElGamal digital signature scheme and the modified versions of the ElGamal signature scheme. The security of the ElGamal algorithms have been tested by using an attack algorithm called baby step giant step algorithm which is applicable for the domain of natural integers and found that the classical ElGamal algorithm is the weakest compared to the other modified versions. The ElGamal scheme in the domain of Gaussian more efficient in respect to time and security. The redactable polynomial scheme has the highest security among these since mathematical complexity of arithmetic modulo a polynomial is high.

The ElGamal algorithm for digital signature is now being applied in various sectors other than banking [9]. It may be applied in case of E-learning, when the study material is intended for a specific group of students then the sender may encrypt the data with digital signature so the intended group of students can only decrypt and get access to the material.

Khater et.al. album signatures for where the voter will sign digitally, and the vote and it will be decrypted by public key securely [6].

Boomija et. al. [8] have proposed the employment of ElGamal like encryption for Cloud Security so that the data stored in cloud would be accessible only to the authentic customers

only who have the right access policy. These are some of the works on ElGamal algorithm which are related to our work.

III. Implementation of E-Banking Transaction System using Elgamal DS

In this section we have implemented DS using Elgamal. The program modules and their relationship is shown in Figure 1. The proposed system consists of Client computer, Web server and Database server proposed system consists of Client computer, Web server and Database server.

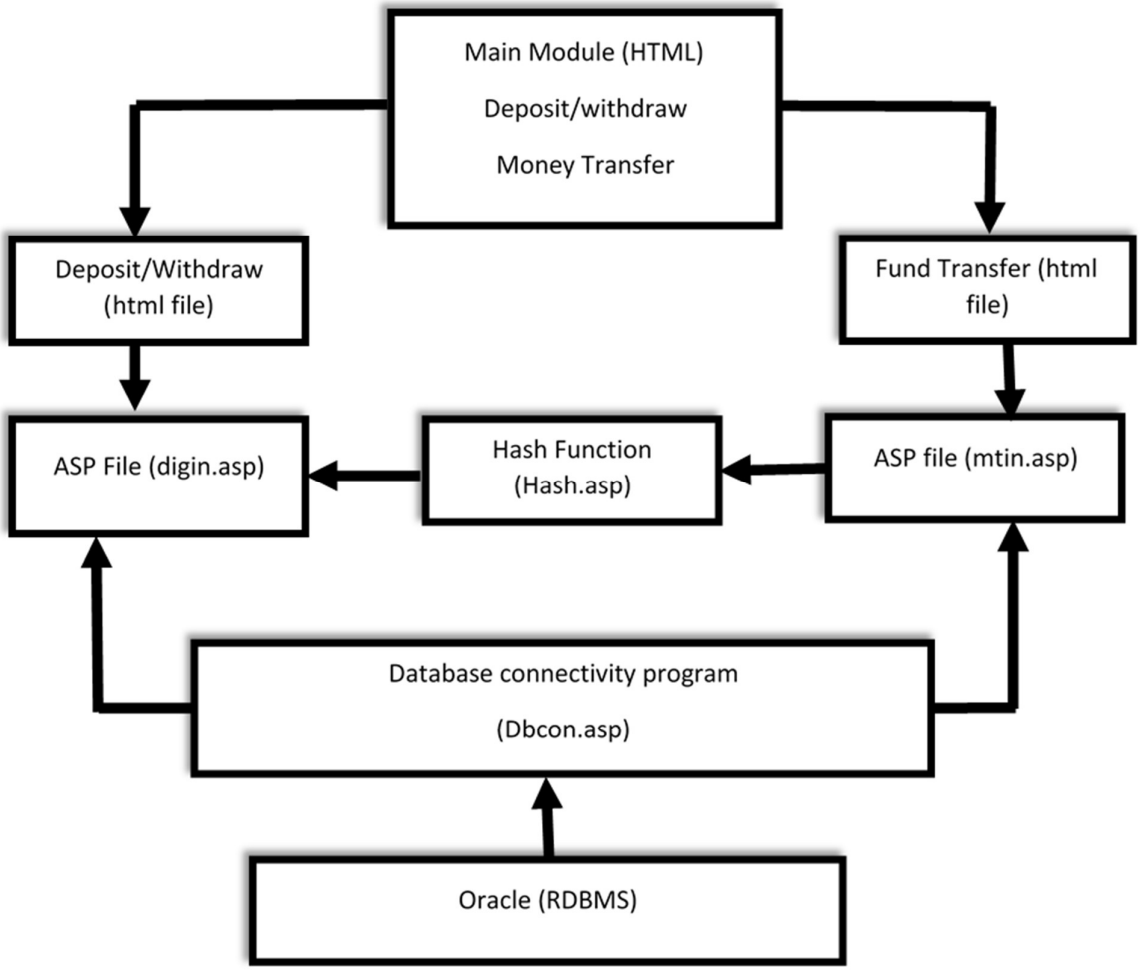


Figure 1. Module and their Relationship for E-Banking System

Client Side: At the client end customer can request for a particular transaction i.e., for deposit, or withdrawal or fund transfer, and the message is generated by giving SQL statements accordingly. Actually, SQL statements are defining the transactions. Before sending the message to the bank's server, the message is encrypted. Then using suitable hash function over the encrypted message, the signature is generated using Elgamal algorithm. The signed encrypted message is sent to the bank server for transaction. The flowchart for client-side application program is given in Figure 2.

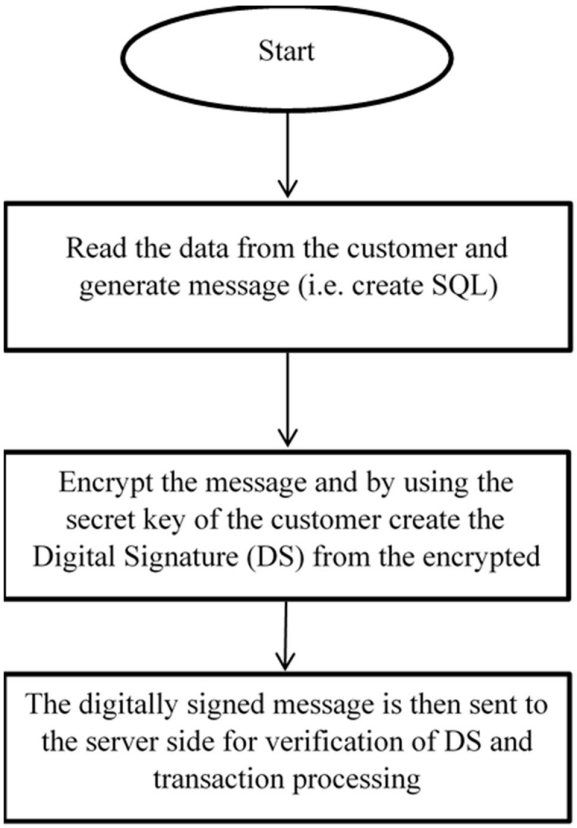
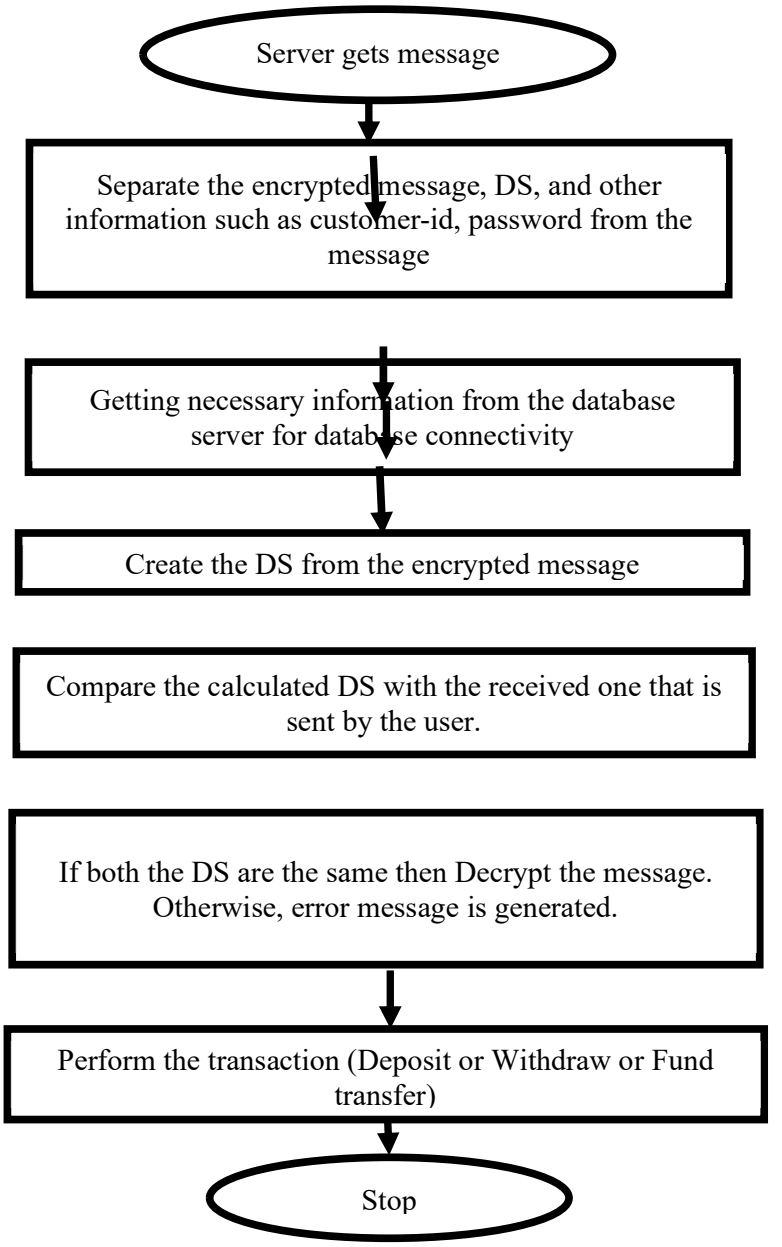


Figure 2. Flowchart for Client-Side Application

Database Server: Database server contains the information about the customer and their transaction. Database server can be connected with the web server by using a connection string. The web server gets information from the client, and checks the message and sends to the database server for execution. The result of the execution of the database transaction is sent to the client via the web browser.

Web Server: This side receives the client message and separates the DS from the message and again recalculates the digital signature by hashing over the received encrypted message. If both the digital signature values are same, then the message is okay and transaction is performed else error message is sent to the client to inform that the message is being changed during communication process between the client and the server. The flowchart for server-side application program is given in Figure 3.



Following program segment will run in server side of our proposed system

Mtin.asp: This is the server-side script for the fund transfer transaction, This ASP program segment is also using the dbcon.asp and hash.asp file. The dbcon.asp and hash.asp file is already defined in the server-side program segment for Deposit and Withdrawal transaction.

Hash.Asp: This function is used to calculate hash value (message digest). This function is used for any type of transaction.

Dbcon.asp: This file is used to establish database connectivity between the database server and web server.

IV. Conclusion

Security is the most important pillar on which entire E-Banking transactions are dependent. Achieving security for an E-Banking System is not an easy task it is a continuous process and

Server gets message from client Separate the encrypted message, DS, and other information such as customer-id, password from the message Getting necessary information from the database server for database connectivity Create the DS from the encrypted message Compare the calculated DS with the received one that is sent by the user. If both the DS are the same then Decrypt the message. Otherwise, error message is generated. Perform the transaction (Deposit or Withdraw or Fund transfer) Stop serious participation of customer and bankers are very important. The system developed by us will take care of every situation of a transaction processing including if the balance is less than the amount to be withdrawn, the transaction will show the appropriate error message without halting the computing system and the transaction will be rolled back. Though the system has been developed for most common types of transactions in E-Banking environment, it may be extended for any financial service institution in E-Commerce environment implementing confidentiality, authentication, integrity and non-repudiation of message. The level of security of the proposed system can be strengthen further using complex hash functions in the implementation of DS, in addition to use of long password.

V. References

[1] Karforma S.(2005) , A study on the application of cryptography in e commerce , [Doctoral dissertation , The University of Burdwan]. Link

[2] Laryoshyna, V.(2017). Simple implementation of an ElGamal Digital Signature and an attack on it.(Book chapter)

[3] Haratya, R. A.(2006)A Comparative Study of Elgamal Based Digital Signature Algorithms. *Journal of Computational Methods in Sciences and Engineering* 6 (2006)S147.*IOS Press(con)*

[4] Laryoshyna, V.(2017). Simple implementation of an ElGamal Digital Signature and an attack on it.(Book chapter)

[5] Haratya, R. A.(2006)A Comparative Study of Elgamal Based Digital Signature Algorithms. *Journal of Computational Methods in Sciences and Engineering* 6 (2006)S147.*IOS Press(con)*

[6] Sultana,R. (2021). A Survey on Digital Signatures. *International Journal of Research Publication and Reviews,* Vol (2) Issue (2) (2021) Page 279-288.

[8] Roy. A. (2012). A survey on digital signatures and its applications. *Journal of Comp. and I.T.* Vol. 3(1&2), 45-69 (2012).

[9] Khater (2018). Blind Signature Schemes based on ElGamal Signature for Electronic Voting: A Survey. *International Journal of Computer Applications* (0975 – 8887) Volume 180 – No.30, April 2018

[12] Banerjee, S.(2015). Object Oriented Metric Based Analysis Of Elgamal Digital Signature Algorithm For Study Material Authentication. International, *Journal of Science Technology and Management* Vol. No.4, Special Issue No. 01, September 2015.

[10]Iswari N. M. S.(2016) Key Generation Algorithm Design Combination of RSA and ElGamal Algorithm. *2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*, Yogyakarta, Indonesia(con)

[11] Boomija, M.D. (2016)Secure data sharing through Additive Similarity based ElGamal like Encryption. *International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics* (AEEICB16) (con)