Research Journal of Recent Sciences ISSN 2277-2502
Vol. 4**(IVC-2015),** 53-59 **(2015)** *Res. J. Recent. Sci.*

Prevention Technique from Hackers and Trackers in on-line-Transactions

Kumar Narander and Chaudhary Priyanka
Department of Computer Science B.B.A. University (A central University), Lucknow, INDIA

Available online at: www.isca.in, www.isca.me
Received th 2015, revised th 2015, accepted th 2015

Abstract

With the advancement of electronic commerce technology and the use of credit card and other types of on-line–transaction facilities has increased in present modern era. In electronic commerce system, credit card is the most prominent idea due to development of the information technology around the wide world. Offline and online both accepted mode are used in present time. Credit card and on-line–transactions is becoming most common payment mode for providing cashless shopping in all over countries or world. It will be provide a convenient approach for online purchasing, payment bills etc. As becoming credit is convenient way for purchasing, fraud are also rising similar way. To distinguish fraud and genuine customer in such extremely sparse data environment is becoming more and more challenging. This paper provides the Prevention Technique from Hackers and Trackers in on-line-Transactions and verification also. To detect the fraud on credit card as well as other on line facilities which are provided by the different companies or organizations is significant for companies and their customers. It has not been prevented fraudulent transaction form being exonerated and the company must gain this type of the financial value of transaction. To minimize penalty of companies that is associated with higher cost and its interest rates also cause of unauthorized access.

Keyword: Credit/Debit Card, on line shopping, unauthorized access, security.

Introduction

All On-line transaction is executed through the internet with the help credit/debit card. To make a secure connection between each customer and the retailer, there are number of methods have been proposed. Online transaction fraud is defined as it is commit fraud or theft through payment card system such as credit card or debit card. Its main objective is to achieve to get goods without any type of payment. In the present time online transaction fraud has became crucial issues and also create more and more problem for credit card. Wherever they have been using normal process for detecting credit card frauds, they cannot achieve goal. To solve this problem, there is a need to develop a model for credit card fraud detection in the academic or business organizations currently. From the few decades, the way of fraud has been suddenly changed because of the development of technologies. Now that time credit Card Fraud is one of the bigger Problems in the field of business and in the field of commercial.

SSL is useful for security in Web trafficking. Security includes three type of element such as confidentiality, authentication and message integrity and these security elements is performed by the use of this type of technique such as cryptography, digital signatures, and certificates in SSL.

In this paper, we have proposed modify RSA algorithm to the bit stuffing its main objective is to be enhancing security level in online transaction.

Related work: Plastic money hoax such as Credit card etc are committing as crime when it usage in networking based transaction. Rahimi A., et al proposed a technique Iris authentication for identify theft in e- commerce transaction. Iris pattern are unique for all individual and it is most secure biometric technique that is performed by the use image processing and customer's secure transmission[1]. EMV is technique that has been secure credit and debit card transaction authenticated by both card and customer. It is possible through a cryptographic code digital signature and entry of a pin. A model is developed in which we describe a protocol flaws that allows to criminal, it uses a card to make for payment without knowing the card's pin[2]. BOAT algorithm is developing to construct efficient fraud detection system which is combination of classification and clustering technique[3]. An algorithm is implemented to distinguish the existence of outliers from a vast data with the help of an online revising is described by[4]. A multiple encryption technique has been developed for secure transaction system by which there are improve the security level of confidential data[5]. A Hierarchy safety control mechanism model is proposed for improving the security of SET protocol with a bring-in electronic business transaction certificate authority which solves these problems[6]. An algorithm is proposed which integrate this type of technique such as genetic algorithms, immune computing, crossover and mutation functionary and fuzzy systems that protect the diversity and expansion of candidate objects. With the use of intelligence techniques for computation[7] in cryptography, there is great improvement in the security levels of group of candidate. A Hidden Markov Model (HMM) model has been proposed in[8] to

sequence the operation in the processing of credit card transaction. If HMM accepted an incoming credit card transaction to validate the transaction with high probability. If it is not then card is not valid and considered to be fraudulent transaction. A new multilayered detection model has been proposed which is entirely based on data-mining technique which is deal with real social relationships and it finds spikes in replicate and finally assigns fishy scores that help to identify the fraud in the system [9]. A hybrid technique based model has been proposed for detecting credit card fraud is discussed by[10]. A probabilistic based model has been introduced for detecting Credit Card System in Online Transactions that is discussed by[11]. A parameterized optimization based model for improving credit card fraud detection that is discussed by[12]. A HMM based model has been proposed with including of several fields such as user profile and it also include only spending profile and the simulation results that are shows the improvement in True Positive and True Negative rates as well as also decreases rate in the form of False Positive and Negative[13].

Overview of SSL: SSL a very popular encryption technology, it is not a payment protocol and now a day's virtually all credit card transactions are encrypted using SSL. It is provide only secure communication between user and retailer. SSL is data exchange protocol that has provided privacy in data between two members such as internet application and server authentication. SSL protocol uses two types of keys for encrypting data first one is public key that is accepted by everybody and further one is private key that is accepted by only to the recipients of the message. SSL protocol allow to user to authenticate the identity of the retailer using digital certificate.

SSL is located within TCP and HTTP protocols. HTTP is standard encrypted communication mechanism that is modified in HTTP (Secure) and it is achieved by HTTPS protocol. SSL protocol standard allows to the concerned components that they have negotiated the encryption, authentication, and integrity technique in use[14]. SSL provide a safe communication within a client and a merchant and it is developed by Netscape[15]. SSL provides three types of cryptography algorithm. The first one is known as authentication that provides permission to the client for identifying the server and also provides permission to the server for identifying the client. Digital certificates for authentication are used by servers in SSL protocol[16]. To performing this type of operation, RSA algorithm is used in this operation. The second one is confidentiality that provides the communication confidentiality between the client and server. The last one is Integrity that has been used for ensuring the integrity of the data across snooping. To performing this type of operation message digest is used and message digest perform this function by the use of checksum[17]. SSL there provide types protocols, which is developed by the above three types of algorithms such as Handshake protocol, Record protocol, and the Alert protocol.

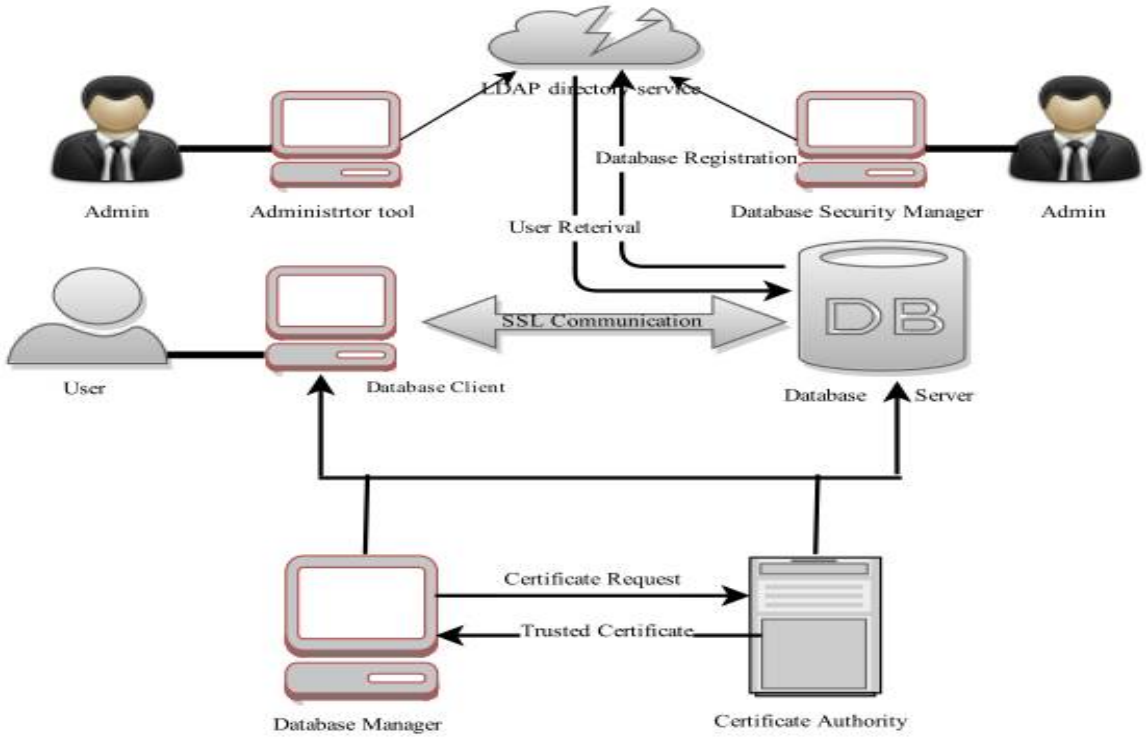


Figure-1
Security Management through SSL

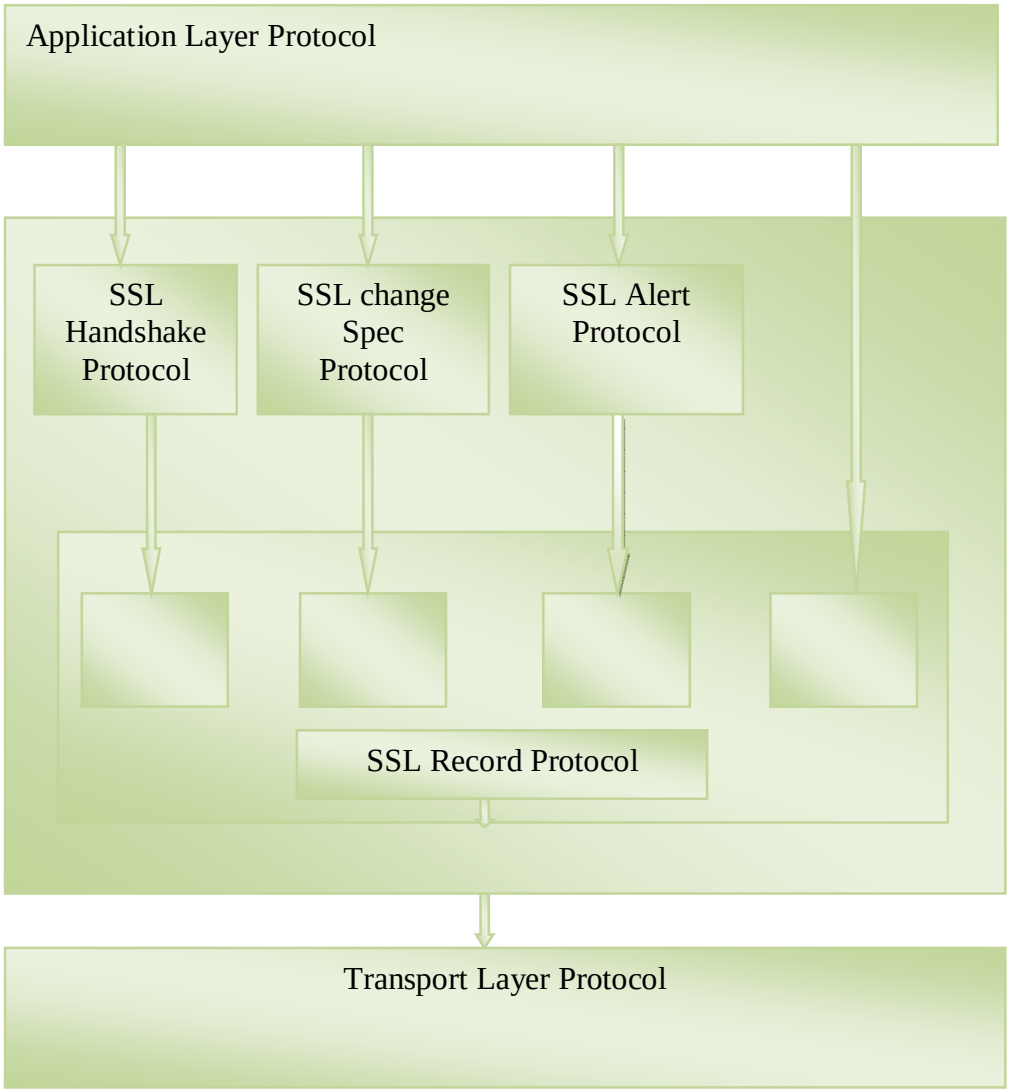


Figure-2
Secure Socket Layer

By the use of SSL protocols there are implement a secure way within the client and the server. SSL record protocol is receive algorithm and key information by which client and server are enables[18]. After completion of handshaking Record protocol is takes place. Record protocol is responsible for all data transfer. It built data path between servers and receivers. Before sending the data it encrypts the data. If any parties find out any type of error it commits an alert that containing the error. This type of operation is handled by the Alert protocol.

Methodology

Proposed Modified RSA algorithm for authentication: Step 1. Choose two prime number primep and primeq and compute their production using bit stuffing method.
Step 2. Compute and find their modulus n= Product of primep and primeq
Ø(n)=(primep-1)(primeq-1)

Step-3. Choose an integer enc that is encryption key for encryption

Where 1<enc<ø(product of primep and primeq), gcd(enc,ø(product of primep and primeq))=1

Step-4. For finding a decryption key dec they have solve the following way

enc.dec=1 mod ø(product of primep and primeq) and 0 ≤ dec ≤ product of primep and primeq

Step-5. Encrypt each message Mess, with the using of public key Ciphertext= $Mess^{enc}$ (mod n)

Step 6. Stored value of Cipher text copy into a BitStuff and add BitStuff into Ciphertext i.e. Ciphertext'=Ciphertext+Bitstuff (if

bitstuff digit containing more than one digit then add these digit and convert into the one digit)

Step-7. Now remove number at receiver side as Ciphertext=Ciphertext`-BitStuff and acceptor decrypts the message with the following order

Mess =Ciphertext ^{dec} (mod n).

Results and Discussion

The below figures defined the implementation of proposed algorithm with a number of different text data values and sizes of a wide range. The encryption time represent is known as, the time is taken for generating a cipher text from plaintext and decryption time represent is known as, the time taken for generating plain text form the cipher text. The algorithm which is proposed in this paper, has taken time to encrypt the data is shown in figure-6. And to decrypt the data is shown in figure-7. In this algorithm we modify RSA algorithm through the stuffing bit which increase the level of security.

In Figure-8, the results shows that time that is taken for the encryption or decryption process by Proposed Algorithm are less than encryption or decryption time of compared existing algorithm[19]

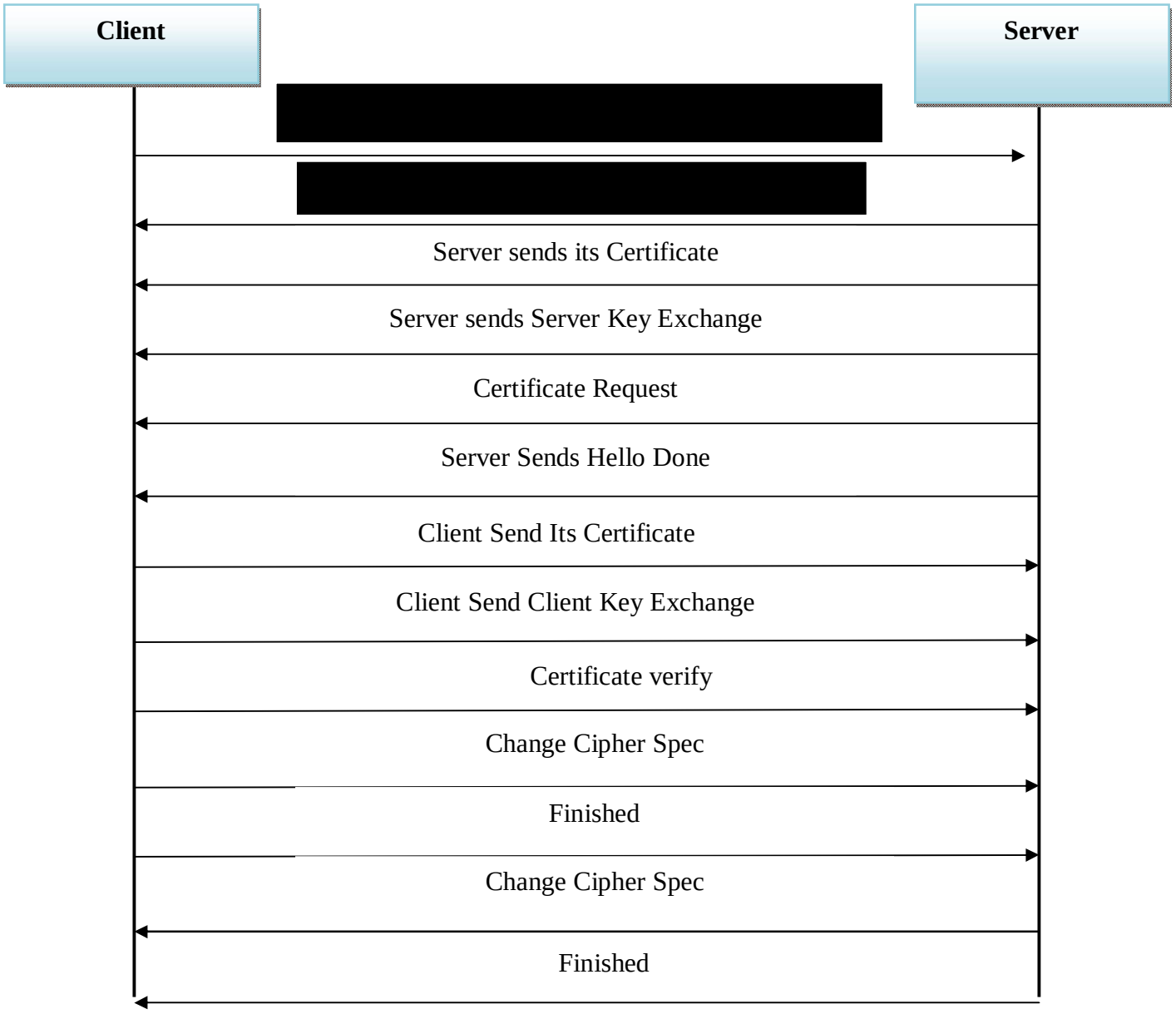
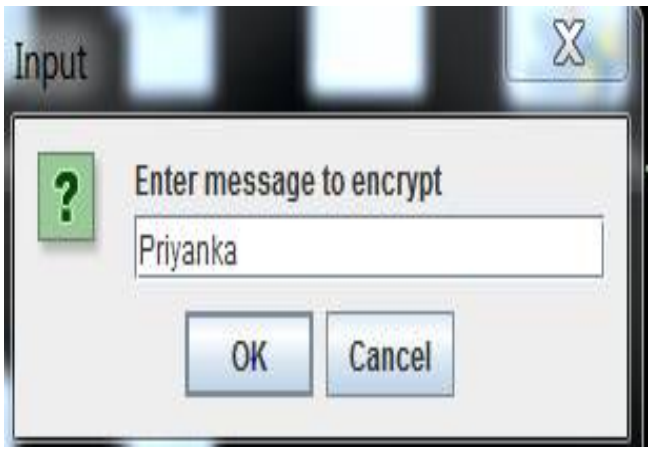
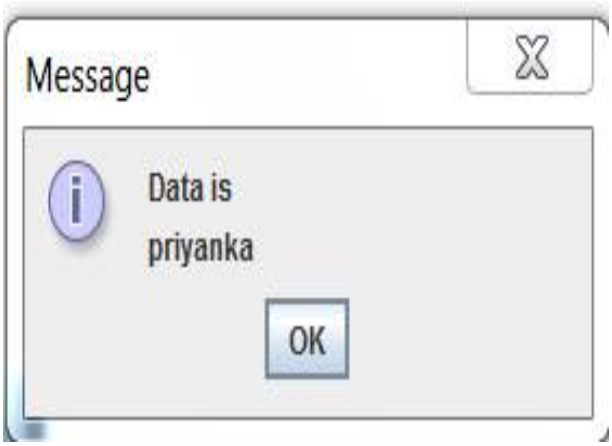


Figure-3
Handshake Protocol





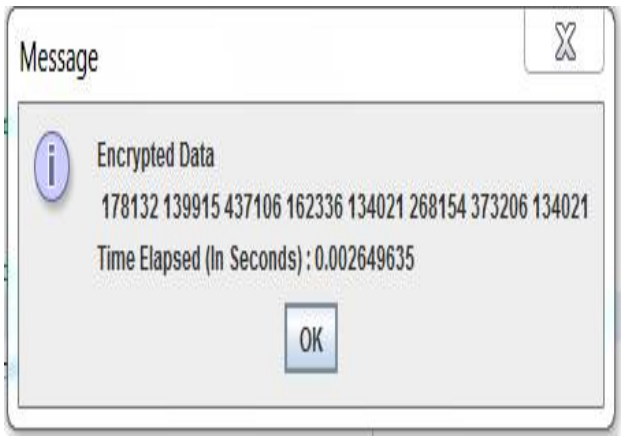


Figure-4
Encrypted Data

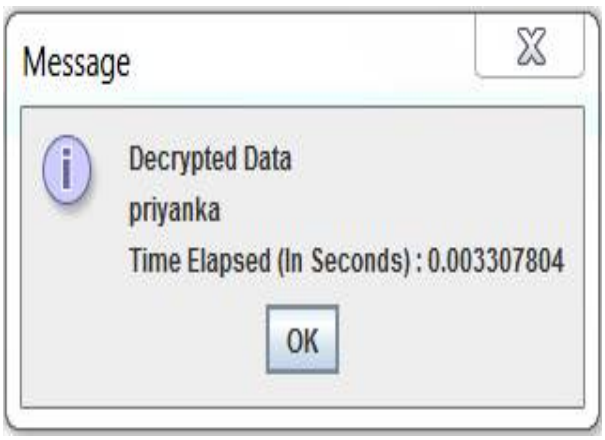


Figure-5
Decrypted Data

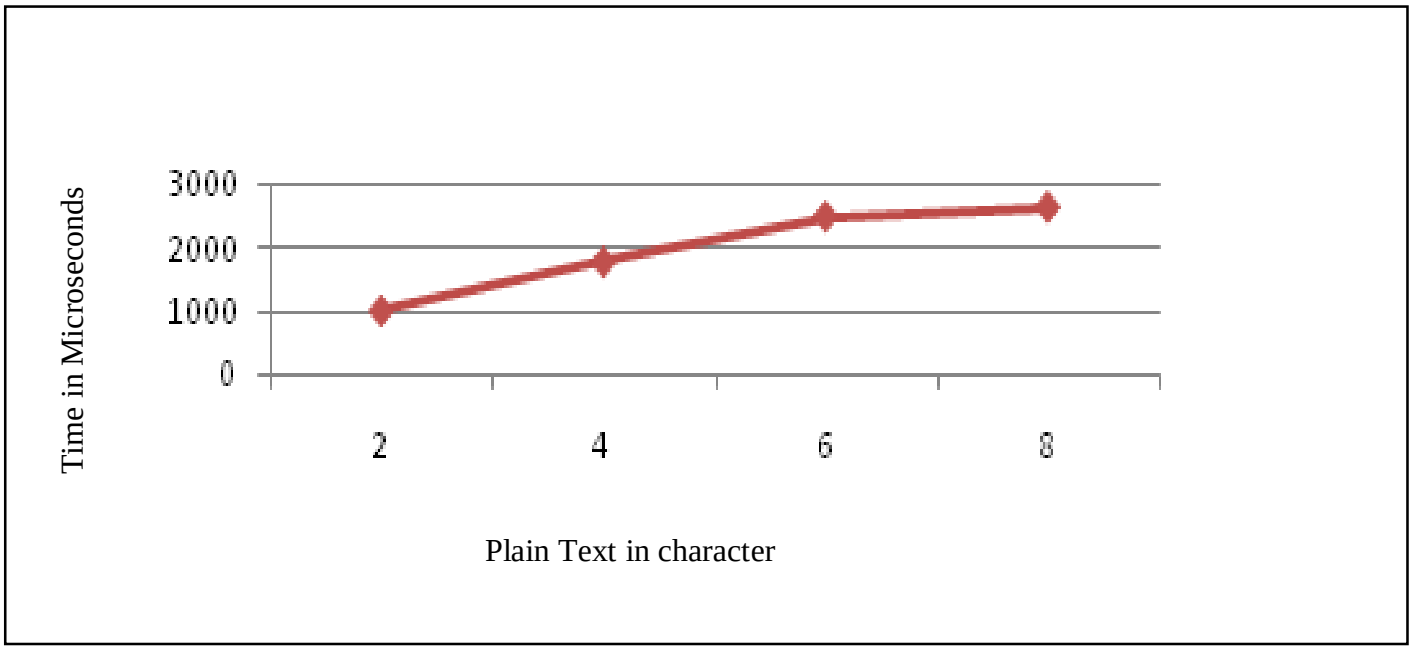


Figure- 6
Time taken for Encryption

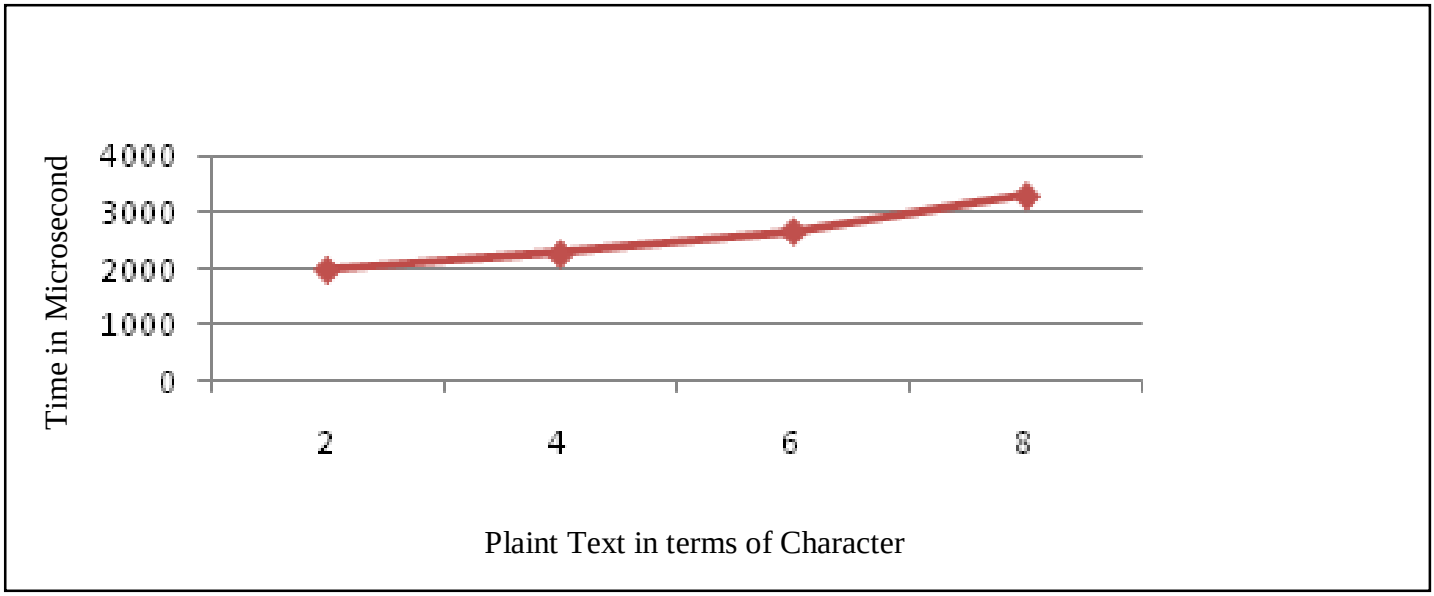


Figure-7
Time taken for Decryption

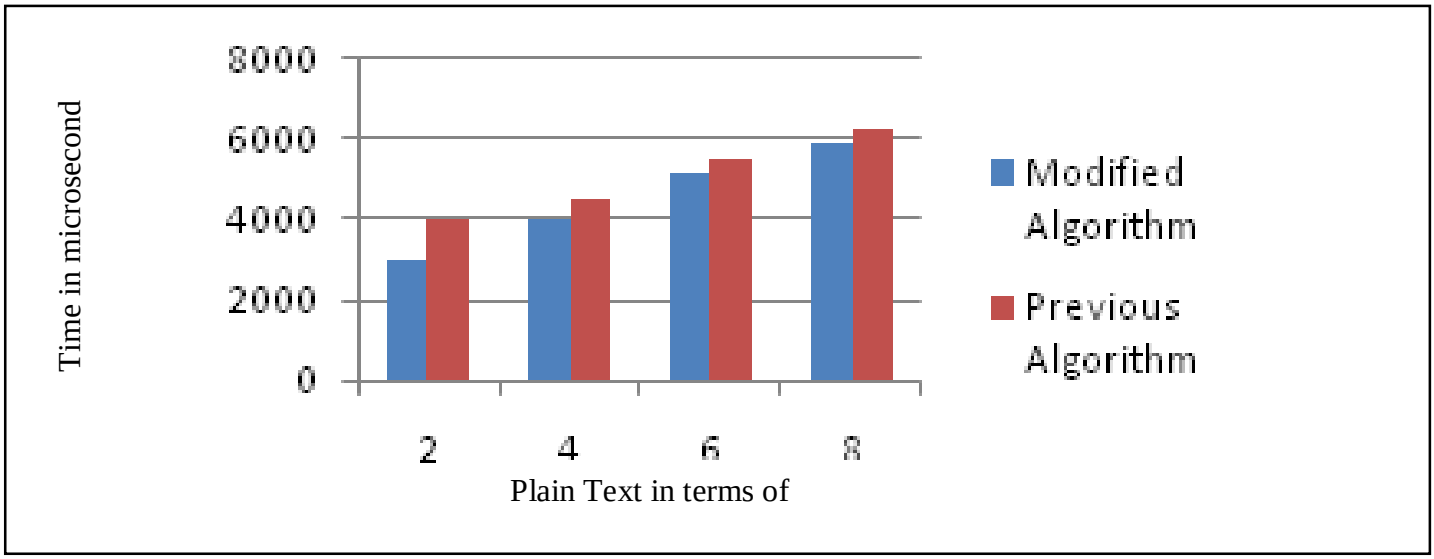


Figure-8
Execution Time (in microseconds) Comparison between Existing Algorithms with Proposed Algorithm

Conclusion

In this paper we have designed an algorithm for improving a security level for communicating between the client and the server in SSL. The RSA algorithm has found several types of liabilities that have been exploited to the continuity, so these types of liabilities, Possibilities of hacking of the algorithms is increased. So, there is a need for designing security technique which is to prevent the exploited discontinuity and improve level of security. In this paper, we have implemented modify RSA algorithm which integrate bit stuffing into a particular algorithm. With the implementation of this algorithm, trespasser cannot access data in easily manner because this bit stuffing method increase level of security. So, this technique improves the security level of the algorithm thus expanding its range with a trusted user.

References

1. Rahimi A., Mohammadi S. and Rahimi R., An efficient Iris authentication using chaos theory-based cryptography for e-commerce transactions, *Internet Technology and Secured Transactions, International Conference for ICITST 2009*, 1-6 **(2009)**

2. Murdoch S.J., Drimer S., Anderson R. and Bond M., Chip and PIN is Broken, *IEEE Symposium on Security and Privacy (SP)*, 433-446 **(2010)**

3. Sherly K.K., Nedunchezhian R., BOAT adaptive credit card fraud detection system, *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 1-7**(2010)**

4. Lee, Yuh-Jye et.al., Yeh, Yi-Ren, Wang, Yu-Chiang Frank, Anomaly Detection via Online Oversampling Principal Component Analysis, *IEEE Transactions on Knowledge and Data Engineering*, 1460-1470 **(2013)**

5. Himanshu Gupta, Vinod Kumar Sharma, Role of multiple encryption in secure electronic transaction, *International Journal of Network Security and Its Applications (IJNSA)*, **3(6)**, 89-96 **(2011)**

6. Zhang Boping and Shang Shiyu, An Improved SET Protocol, *Proceedings of the 2009 International Symposium on Information Processing (ISIP'09)*, 267-272 **(2009)**

7. Anjali Dadhich, Dr. Surendra Kumar Yadav, Evolutionary Algorithms, Fuzzy Logic and Artificial Immune Systems applied to Cryptography and Cryptanalysis: State-of-the-art review, *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, **3(6),** 2112-2120 **(2014)**

8. Avinash Ingole, R.C. Thool, Credit Card Fraud Detection Using Hidden Markov Model and Its Performance, *International Journal of Advanced Research in Computer Science and Software Engineering*, **3(6)**, 626-632 **(2013)**

9. Alka Herenj, Susmita Mishra, Secure Mechanism for Credit Card Transaction Fraud Detection System, *International Journal of Advanced Research in Computer and Communication Engineering*, **2(2),** 1244-1248 **(2013)**

10. Krishna Kumar Tripathi et.al., Lata Ragha, "Hybrid Approach for Credit Card Fraud Detection", *International Journal of Soft Computing and Engineering* (IJSCE), **3(4),** 8-11 **(2013)**

11. S.O. Falaki et.al., B.K. Alese, O.S. Adewale, J.O. Ayeni, G.A. Aderounmu and W.O. Ismaila, Probabilistic Credit Card Fraud Detection System in Online Transactions, *International Journal of Software Engineering and Its Applications et.al.*, **6(4),** 69-78**(2012)**

12. A. Prakash and C. Chandrasekar, A parameter optimized approach for improving credit card fraud detection, *IJCSI International Journal of Computer Science*, **10(1),** 360-366 **(2013)**

13. Ranjit kumar, Sandeep Raj, Design and Analysis of Credit Card Fraud Detection Based on HMM, *International Journal of Engineering and Innovative Technology (IJEIT)*, **2(3),** 332-334 **(2012)**

14. Narander kumar, Priyanka chaudhary, Minimize cyber losses in cyber world through the optimization technique, *Ïntenational journal of computer science*, **96(20),** 18-22 **(2014)**

15. http://docs.oracle.com/cd/E17904_01/core.1111/e10105/sslconfig.htm **(2015)**

16. Cisco Systems, Introduction to Secure Sockets Layer.

17. H. Otrok, Security testing and evaluation of Cryptographic Algorithms **(2003)**

18. Otrok H. Haraty and R. El-Kassar A.N., Improving the Secure Socket Layer Protocol by modifying its Authentication functions, *Automation Congress, 2006. WAC '06. World*, 1-6 **(2006)**

19. Parshotam, Rupinder Cheema and Aayush Gulati, Improving the Secure Socket Layer by Modifying the RSA Algorithm, *International Journal of Computer Science, Engineering and Applications (IJCSEA)*, **2(3),** 79-86 **(2012)**