Secure Data Access Scheme using encryption and steganography based on secure image based password

[1]Anuja Patole, [2]Dr. Archana Lomte
[12]Department of Computer Engineering, Bhivarabai Sawant Institute of Technology & Research, Pune, India.

Abstract : In this paper, proposed system doing introduce a secure data scheme with cryptographic primitives for data access from the database server. With a formally defined adversary model and security analysis, the proposed scheme is proven to be both accurate and secure via mixing of encryption, steganography and splitting methodology. It provides strong data storage robustness and communication security to registered users during data uploads and downloads important data. On the other hand, the performance evaluation shows the practicability of our proposed secure data transmission scheme, as the total computation cost is acceptable. In modern day technology, the Information Society is at risk. Passwords are a multi-user computer systems usual first line of defence against intrusion. A password may be textual with any combination of alphanumeric characters. But no authentication protocol is fully secured against todays hackers as all of them are Static in type. Dynamic authentication protocol is still a theoretical concept. In this paper covered the idea of generating an efficient algorithm that can work as the final in the Dynamic Password Authentication system.

Index term: Password Encryption Process, Image Steganography, Image Process Management, Network Security Management, OTP.

I. INTRODUCTION

With the growth different types of network digital images are being exchanged over the networks. The basic need of every growing area today's world is communication. Everyone wants to protect the information of work to be secret and safe. The rise of the internet, the most important factors of information technology and communication has been the security of information. In our day life we have used many insecure pathways for sharing and transferring information using telephonically or internet. However at a certain level it's not safe. Cryptography and steganography are two methods that use information in order to cipher or cover their existence respectively which could be used to share and transfer information in a concealed manner. Cryptography is a technique includes modification of a message for security the secrecy communication. Nowadays, to encrypt and decrypt data in order to protect the message secret many different methods have been developed.

In cryptography it's always clear to intermediate person that the message is encrypted form by an encryption key which is known by sender and receiver only and without using encryption key the message could not be accessed. However, these methods are not enough to protect the contents of a message secret due to another technique is used with cryptography that is called steganography. Steganography is the art and science of invisible communication of message and the secret message is made to hide in cover image and person cannot be seen any message hidden in the image. The cover image containing the secret data is then transferred to the recipient. The receiver is able to extract the message with the retrieving process and secret key provided by the sender.

Problem Statement:

Exploitation of password (user account) is one of largest issues in cyber security as it is an easy way to gain the unauthorized access from the attacker. Today's process is the single widespread form of attack that penetrates a network, system, or resource with or without the use of tools to unlock a resource that has been secured with a password is known as password cracking. There are many reasons that make passwords cracking possible. These reasons include human factors such as short or easily-guessing passwords, usage of weak algorithms. So our proposed system is Authentication by Encrypted Negative Password based on SHA algorithm and encryption technique.

II. REVIEW OF LITERATURE

In [1] the problems are more increases with online shopping and online payment, the customer protection is most important during the online transaction that wants privacy and trust between different geographical locations or countries [1]. There is increasing attacks and threads over online shopping or online payment because of insecurity, un-authorization access lack of customer's protection and trust which are vital elements for a successful online transaction between customer to customer, organization as well as individual.

In [2], report he analysis and review major problem faced by customer in an online transaction or shopping is security. From survey report, it is mostly happening transaction base on e-commerce have been constrained by security. In addition he analysis, consumers are concern about their privacy when their personal information are required to facilitate transaction besides, potential risks are also posed to those using credit cards to make purchase online. Secured system with privacy is needed to enhance online shopping since consumers cares for their privacy and security. Furthermore, [2] the author explain online shopping paves way to fraudulent act and unworthy credit orders which is also attributed to unsecured services. Trust also plays an essential role on consumer's choice for online purchase.

In this paper the author [3] explain that trust is most important in online businesses environment determines consumer's willingness to engage in online business area. He implements security such as the use of digital signature and certificates are mostly used and more secure in controlling or avoiding risk of fraud for online-based transactions [3].

In another study [4], explain the e-commerce for goods services during online transaction. It was pointed out that security, protection policy and as well as reliabilities of companies are major barriers to online shopping. However, consumer's behavior towards online shopping includes and not limited to [5]; concern over unauthorized sharing of personal information, unsolicited contacts from the online retailer, and undisclosed tracking of shopping behavior. Besides, system security-consumers who are concern about illegal bridging technological protected devices to acquire consumer's personal, financial or transaction-related information. Concern over online retailer fraud cause by purposeful misrepresentation or non-delivery of goods paid for are among the potential threat over online purchase.

Improved security system for online shopping could reduce miss-behavior of consumers' with increase intention for online transaction [6]. Here user disposing of the customer's personal detail and credit card information during and after online transaction should be avoided as it gives more room for illegal use of customer's information. Once information get then attacker misuse that information for other purpose. Trust in online transaction could be enhanced through policies that incorporate legal, technical, rigorous standards for security, data protection and as well as certificates of independent trusted third parties [6].

In this study author improved security in online shopping could widely use and encourage consumers to engage in e-commerce deal as well as its awareness and role among Libyan economic units. Consumers feel relaxed to use online medium when their capital and information are properly protected [7].

In addition, online portal is encourage trustworthy relationship between customer and online portal in order to increase and attract consumers to online transaction by ensuring that every transaction is kept within the scope of agreement [8]. Owing to the need to facilitate e-commerce transaction in Libya we hereby proposed that efficient measures for effective implementation of e-commerce transaction in Libya economic developments should integrate web-based infrastructures.

III. PROPOSED OVERVIEW

In the proposed system, information which is submitted by the consumer to the online website at merchant's site is minimized by providing only minimum information. It will only verify the payment made by the consumer from its account. This is accomplished by the introduction of a central Certified Authority (CA) and combined application of visual cryptographic Steganography and technique. The information which is obtained by the merchant will only validate receipt of payment from authentic consumer. It can be in the form of account number related to the card used for shopping.

IV. SYSTEM ANALYSIS

We implement these system for avoiding the network security threads occurring when people online transaction. We analysis this system using the following points: In this paper we use the following algorithm for implementing the secure system.

1. Blowfish Algorithm

In this system we implement the blowfish encryption algorithm to encrypt the providing information during the online payment. This algorithm is more secure rather than other encryption algorithm. Blowfish 64-bit block cipher with a variable length key. This algorithm is widely used because it operation process requires less memory and more secure. It uses only simple processing steps, therefore it is easy to implement. It is fast algorithm process to encrypt the given customer data. It requires 32 bit microprocessor at a rate of one byte for every 26 clock cycles.

2. Image Uploading Algorithm

In this project image uploading is must for creating the secret image for hiding the information for security purpose. Firstly you have to add packages for accessing the methods and functions. Then you have added the drives for connecting the database. Then you create the connection link for database. Then you put the proper sql query for storing the image into database.

3. Mail sending algorithm

Here we send the mail using the API (javax.mail). You need a SMTP (Simple Mail Transfer Protocol) server.

4. OTP generation

Here OTP (One time password) in a typical two-factor authentication application, user authentication proceeds as follows: User authentication purposed we used the OTP as login phase, once authentication success then we used another OTP during online payment transfer.

V. CONCLUSION

We use visual Cryptography to provide secure transaction during online shopping. It secures the customer confidential information as well as merchant credential. Prevent misuse of data at bank side by Admin Application. This method is mainly concerned with preventing identity theft and prevents phishing. It also was providing customer data security.

We use encryption technique using blowfish algorithm and steganography to hiding the data to provide secure transaction during online transaction. It secures the customer confidential information as well as merchant credential and prevents misuse of data at bank side by Admin Application. This technique is mainly implementing with preventing identity theft, providing customer data and also prevents phishing.

VI. ACKNOWLEDGMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide Dr. Archana Lomte for him time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

REFERENCES

[1] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, “Passwords and the evolution of imperfect authentication,” Communications of the ACM, vol. 58, no. 7, pp. 78–87, Jun. 2015.

[2] M. A. S. Gokhale and V. S. Waghmare, “The shoulder surfing resis-tant graphical password authentication technique,” Procedia Computer Science, vol. 79, pp. 490–498, 2016.

[3] J. Ma, W. Yang, M. Luo, and N. Li, “A study of probabilistic password models,” in Proceedings of 2014 IEEE Symposium on Security and Privacy, May 2014, pp. 689–704.

[4] A. Adams and M. A. Sasse, “Users are not the enemy,” Communications of the ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999.

[5] E. H. Spafford, “Opus: Preventing weak password choices,” Computers & Security, vol. 11, no. 3, pp. 273–278, 1992.

[6] Y. Li, H. Wang, and K. Sun, “Personal information in passwords and its security implications,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 2320–2333, Oct. 2017.

[7] D. Florencio and C. Herley, “A large-scale study of web password habits,” in Proceedings of the 16th International Conference on World Wide Web. ACM, 2007, pp. 657–666.

[8] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, “Designing password policies for strength and usability,” ACM Transactions on Information and System Security, vol. 18, no. 4, pp. 13:1–13:34, May 2016.