

Chapter 1

INTRODUCTION

Information has been valuable since dawn of civilization. As access to stored data in computer has increased, information security has become extremely important. Information security is basically a set of procedures implemented to prevent the unauthorized access, abuse, alteration, inspection, destruction or denial of access to knowledge, data, or resources. There are four basic elements that are used in information security to generate sound policy. They are confidentiality, integrity, availability, accountability. Confidentiality prevents disclosure of information to unauthorized individuals or systems. Integrity maintains and assures the accuracy and consistency of data over its entire life-cycle with respect to the end user. Availability ensures that the information will be available when it is needed and accountability adds responsibility and redundancy into the planning and implementation of security policies.

For the creation of a complete information security policy, implementation of network security is essential. Actually physical, communication, emission, computer, and network security together make up the concept of information security. Network security refers to the provisions and policies that are essential to the usability, reliability, integrity and safety of data and network.

Such an online payment system is implemented using steganography and visual cryptography. Steganography and cryptography are chosen because there are most widely used techniques for the protection of confidential information. Visual cryptography is chosen because of its ability to generate shares which enhances customer trust. Here steganography and visual cryptography together minimize information sharing between customer and online merchant but enable successful fund transfer from customer account to merchant's account thereby safeguarding customer information and information misuse at merchant side. The main objective of this technique is to maintain confidentiality and prevent misuse of customer data at merchant side by providing a two layer of security.

Online shopping is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier. Identity theft and phishing are the common dangers of online shopping. Identity theft is the stealing of someone's identity in the form of personal information and misuse of that

information for making purchase and opening of bank accounts or arranging credit cards. In 2012 consumer information was misused for an average of 48 days as a result of identity theft. Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials.

In 2nd quarter of 2013, Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant. However, one must still trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others. In this paper, a new method is proposed, that uses text based steganography and visual cryptography, which minimizes information sharing between consumer and online merchant but enable successful fund transfer from consumer's account to merchant's account thereby safeguarding consumer information and preventing misuse of information at merchant side. The method proposed is specifically for E-Commerce but can easily be extended for online as well as physical banking.

A cryptographic technique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing scheme a secret image is encrypted in shares which are meaningless images that can be transmitted or distributed over an untrusted communication channel. Only combining the k shares or more give the original secret image. Phishing is an attempt by an individual or a group to thief personal confidential information such as passwords, credit card information etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities. The use of images is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both are simultaneously available; the individual share images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. Several solutions have been proposed to tackle phishing. In the proposed solution, information submitted by the customer to the online merchant is minimized by providing minimum information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of steganography and visual cryptography