E-Pay Using Cloud and Steganography For Android Smartphones.

Prof.Thosar Sonali D[1], Mr.Phad Laxman C[2], Mr.Patil Abhishek D[3].

[1] *Prof.Thosar Sonali D, Computer Engineering, Pravara Rural Engineering College, Maharashtra, India*
[2] *Mr.Phad Laxman C, Computer Engineering, Pravara Rural Engineering College, Maharashtra, India*
[3] *Mr.Patil Abhishek D, Computer Engineering, Pravara Rural Engineering College, Maharashtra, India*

ABSTRACT

This paper is aim at creation of a Secure e-Pay Using Steganography with Cloud Approach. In the recent time E-Commerce market has been grown rapidly and with increasing popularity of online shopping.Debit or Credit card fraud are common in these days and personal information security is major issue for customers as well asmerchants and banks in the case of CNP (Card Not Present).So our aim is to create such Software application(for Android Smartphones) which is accessible to all customers who have a valid User Id and Password and to perform their online purchase-payment transaction secularly using steganography with cloud approach. This is an approach to provide a limited information which is necessary for fund transfer during online shopping and enhancing security of customer data and increasing their confidence for online transactions. By using this application customer can perform transaction securely from anywhere without worrying about their privacy of data. In this project we are going to use steganography. It is one of the reliable technique for securing information data. In this project we are going to deal the facts in current online payment system i.e. the transactions which takes place between buyer/customer and online merchant. We provide a real time environment for the system in online payment process. We deal with the methods for transaction in the online fund transfer can be made faster and easier. So that is main goal of project and it is an internet/cloud based computerized approach towards online transaction for e-shopping.

Keywords - *AES Advanced Encryption Standard. CSP Cloud Service provider. CS Cloud server. ENC Encryption. DEC Decryption. SEC Security. IBE Identity based encryption.*

1. INTRODUCTION

Smartphone users are continuously increasing in these days. they often want to purchase products from online shopping, As survey shows number of android smartphone users are more than others. Android Smartphone mobile application is platform, developed by the Open Handset Alliance (OHA). This Android system consists of 4 layers: the Linux kernel, native libraries, the virtual machine, and an application framework .[1] In the android architecture Linux kernel provides basic operating system services and hardware abstraction to the next level software stacks. The Native libraries provides functionalities of multimedia data processing,web browsing, database access, and great flexibility and support for Online transaction such as e-shopping.[1]

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks,which is to provide dynamically scalable infrastructure for application, data and file storage.[2] With the advent of in this technology, the cost of computation and application hosting, content storage and delivery is reduced significantly. There are multiple advantages of using cloud such as cost reduction, large storage capability, great flexibility in this application we are using cloud as Software as a Service (SaaS). In which complete application is offered to the customer, as on demand of service.[3] A single instance of the service runs on the cloud and number of multiple end users are serviced. On the customer's side, there is no need for investment in servers system or software licenses, while for the provider, the costs are less, since only a single application needs to be hosted & maintained.

Today Cloud Software as a Service is offered by many companies such as Google, Sales force, Microsoft, Zoho,etc[4].Online shopping is the retrieval of product information through the Internet and issue of purchase order through electronic purchase request, and making transaction by filling of debit or credit card information and shipping of the product by mail order or home delivery by courier.Common dangers of online shopping are Identity theft as well as phishing.[5] Identity theft is the stealing of someone's identity in the form of confidential information and using that information in wrong way for making purchase and opening of bank accounts or arranging debit or credit cards. Phishing is an illegitimate method or mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account details of credentials.Payment Service, Financial and Retail Service are the most focused industrial sectors of phishing attacks.[6]

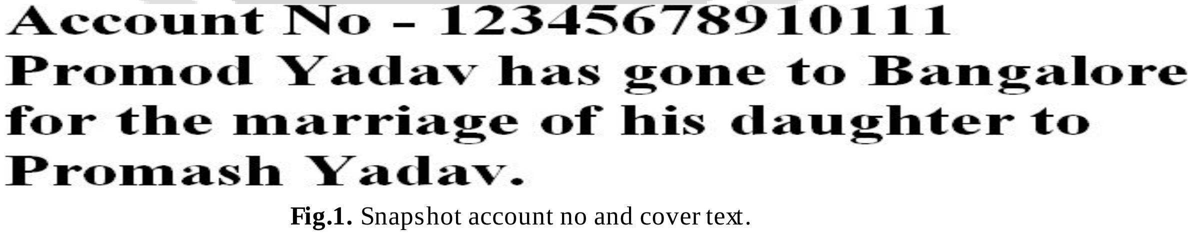
Secure Socket Layer (SSL) encryption restrict the interference of consumer information in transmission between the consumer and the online merchant. However, one must still trust merchant and his employees not to use consumer's information for their own purpose and not to sell the information to others which is extremely unsecure for customers so there is need of system which provide capability and functionality to do transaction securely. In this application, a new method is proposed that includes both steganography and cryptography,[7] which minimizes detailed information sharing between online merchant and consumer but enable successful fund transfer from consumer's account to merchant's account in this way safeguarding consumer information and preventing misuse of information at merchant's side. The method proposed is applied to E-Commerce using Android Smartphones and it also can be easily extensible for other applications like online banking for future use.[7]

2. PROPOSED SYSTEM

The proposed system aims at creation of a "Secure e-Pay Using Steganography." This will be accessible to all user which have a valid 'Password' and 'User id the system provides using Android Smartphones. In the proposed solution, data submitted by the user to the online merchant is minimized by providing minimum information that will only verify the payment made by the said customer from his bank account. This is achieved by the introduction of a central Certified Authority and combined application of Steganography and Cryptography.

The information received by the merchant it can be account number related to the card used for shopping. The information will only validate receipt of payment from authentic customer. The following important functionalities Unauthorized Access is the main tool used by Criminals. Unauthorized access means fack user or any access without the permission of real owner or in charge of the computer, computer system or computer network.

Common techniques like Phishing etc. are the used for unauthorized access. So to prevent this access there is need of system which is more secure, flexible, yet easy to use in general. So the proposed method is very much secure and powerful to provide security in online transaction Fig. Shows transaction method for a proposed system.



Account No – 12345678910111
Promod Yadav has gone to Bangalore
for the marriage of his daughter to
Promash Yadav.

Fig.1. Snapshot account no and cover text.

Fig. 2. Steganographied Image kept by customer.

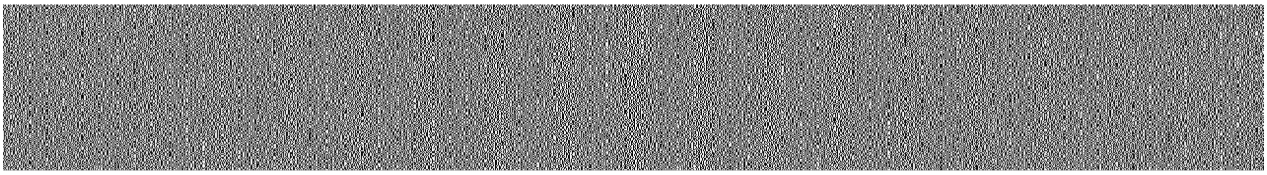
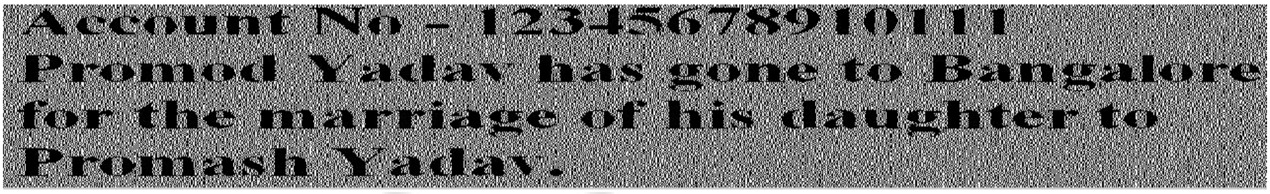
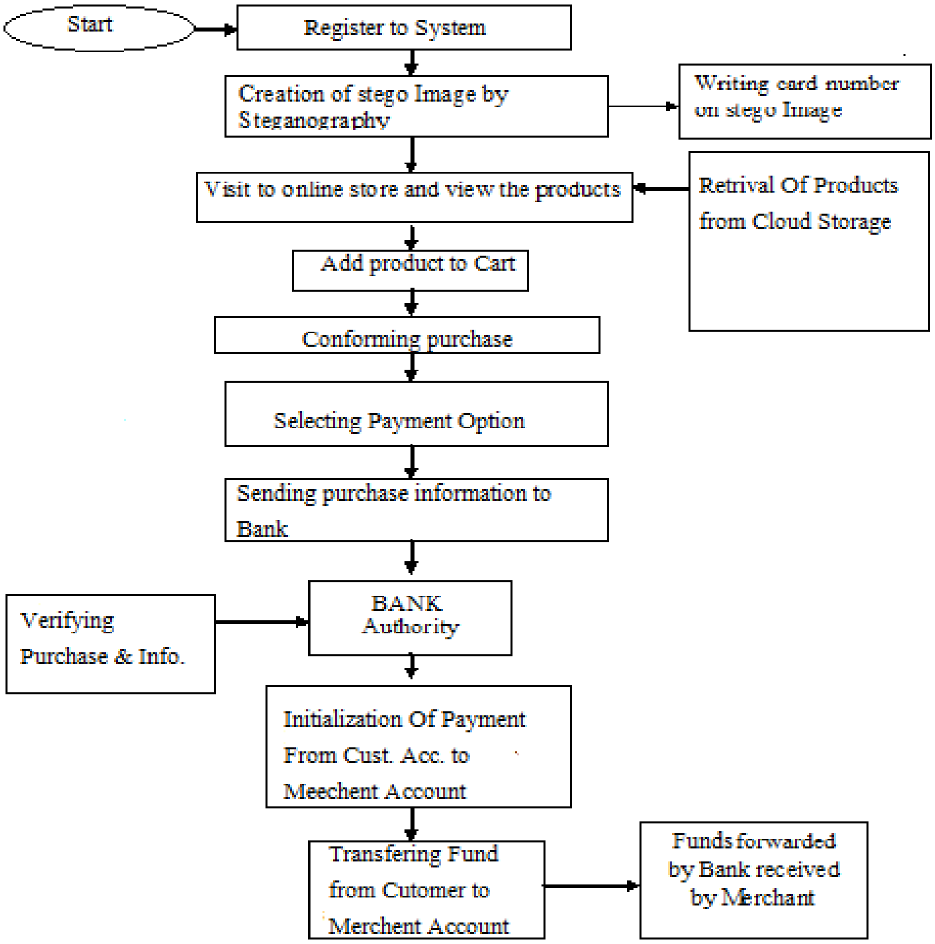


Fig. 3. Generated Cover Image for Sharing.



Account No - 12345678910111
Promod Yadav has gone to Bangalore
for the marriage of his daughter to
Promash Yadav.

Fig. 4. De- Steganographied Image.



Start
Register to System
Creation of stego Image by Steganography
Writing card number on stego Image
Visit to online store and view the products
Retrival Of Products from Cloud Storage
Add product to Cart
Conforming purchase
Selecting Payment Option
Sending purchase information to Bank
Verifying Purchase & Info.
BANK Authority
Initialization Of Payment From Cust. Acc. to Meechent Account
Transfering Fund from Cutomer to Merchent Account
Funds forwarded by Bank received by Merchant

Fig.5. Workflow of System.

In our proposed system of e-pay shopping, user logs in and enters into the online store to view the products or item. When he/she choose the item and add to the cart, he/she will be entering the card number and unique authentication password. This data information will be created as a stego or stegno image using Steganography technique. Steganography will create two shares out of the stegno image. Bank browses user's share and generates the card no which is sent to the cloud database so as to extract the user's PIN (desteganography). Finally fund will be transferred from the bank to the merchant. Workflow of our proposed systemas showin Fig.5.

3. IMAGE BASED STEGANOGRAPHY

All type of digital file formats can be used for hiding information using steganography, but the formats that have a high level of degree of redundancy present in them are more flexible. The redundant bits of an object are those bits that can be changed without the alteration being detected easily. As digital images contain large volume of redundant bits, they are the more popular digital media for steganography. This are relatively easy because an image, being an array of pixels, typically

contains an huge amount of redundant information. An image is a collection of numbers that constitute multiple light intensities in different areas of the hole image. Image based steganography is about exploiting the limited powers of the human visual system (HVS). There are many ways to hide messages within images. The security of stego images are depends entirely on their ability to go unawared,. When working with digital images, the images seems to be large to be transmit on the Internet. Choice of the cover image is an important fact of steganographic technique and thus compression plays a necessary role. Current image formats can be divided into based on two lossy and lossless categories of compression techniques.

Both methods save memory space but have different results. Lossless compression rebuild the original message exactly and thus it is preferred when the actual information must remain intact . Lossless images are more for embedding, since the integrity of the image data is preserved. However, they don't have more compression ratio of an as lossy formats do. the Lossy compression, on the other hand, saves memory but it may not maintain the original image integrity. The positive side of lossy images, in particular JPEG, is that it can achieves extremely high compression, while maintaining fairly good quality .Previously, it was felt that steganography using JPEG file format images is not possible as lossy compression involves reduction of bits and thus data may be lost. One of the major features of steganography is the fact that massage is hidden in the needless bits of an object and since needless bits are left out when using JPEG it was feared that the hidden data would be destroyed.

However, the properties of the compression algorithm have been exploited in order to an evolve a steganographic algorithm for JPEGs Thus it is not necessarily seeming to a human eye that the image has been changed. Lossy compression is preferred in image based steganography technique because it achieve higher compression compared with lossless compression and thus it is more secure and have less chances of detection that of lossless. Steganography not only deals with embedding the secret information inside the digital media or image but also the receiver to whom the information is intentional, must know the method used and would be able to retrieve the information successfully without drawing the attention of a third party that a secret communication is occurs. Following Fig. shows the technique of steganography.

4. CONCLUSION

Thus, we can conclude that a payment system for online shopping is using steganography authentication that provides customer data or information privacy and prevents misuse of data at merchant’s side. The proposed method can be applied for E-Commerce with focuses on area of payment during online shopping as well as physical banking

5. REFERENCES

[1] Jihui Chen, XiaoyaoXie, and Fengxuan Jing, "The security of shoppingonline," Proceedings of 2011 International Conference on Electronic andMechanical Engineering and Information Technology (EMEIT), vol. 9,pp. 4693-4696, 2011.

[2] M. Armbrust et al., “A View of Cloud Computing,” Comm. of theACM, vol. 53, no. 4, pp. 50-58, 2010

[3]W. Jansen and T. Grance, “Guidelines on Security and Privacy inPublic Cloud Computing,” Technical Report Special Publication800-144, NIST, 2011.

[4]L.Ferretti, M. Colajanni, and M. Marchetti, “Supporting Securityand Consistency for Cloud Database,”Proc.Fourth Int’l Symp.

[5]Anti-Phishing Working Group (APWG), “Phishing Activity Trends Report, 2013,”http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf .

[6]J.C. Judge,“Steganography:Past, Present, Future,” SANS Institute ,November 30, 2001.

[7] M. Naor and A. Shamir, “Visual cryptography,” Advances in Cryptograhy: EUROCRYPT’94, LNCS, vol. 950, pp. 1–12, 1995.