https://doi.org/10.46335/IJIES.2023.8.5.9 **e-ISSN: 2456-3463**
Vol. 8 , No. 5, 2023, PP. 42-44

International Journal of Innovations in Engineering and Science, www.ijies.net

Privacy Protection for Cloud Based Online Transaction Using Steganography & Visual Cryptography

Ms.Vaishnavi S. Kshirsagar[1], Prof. N. M. Sawant[2]

[1]PG Student, Department of Computer Science Engineering,
SKN Sinhagad college of Engineering, Korti, Pandharpur, Solapur, Maharashtra, India, Pin-413304,
[2]Assistant Professer, Department of Computer Science Engineering,
SKN Sinhagad college of Engineering, Korti, Pandharpur, Solapur, Maharashtra, India, Pin-413304

vkshirsagar676@gmail.com

***Received on**: 03 April, 2023* ***Revised on**: 08 May, 2023* ***Published on**: 10 May,2023*

***Abstract** –In the present days, we are moving towards modern technologies of cashless transactions. Whenever we are doing online transactions, some data is produced. Day by day the production of data is increased to manage such data cloud computing is the best solution, it is based on pay as per use strategy, but while sharing the personal data in cloud environment security is important issue and this can be solved by using Steganography and visual cryptography. In this study, we are providing secure solution for the online transaction with the combination of steganography and visual cryptography by introducing new certified authority in between the customer and merchant. The certified authority prohibits the merchant to access and store the customer's confidential data.*

***Keywords**-Steganography, Cryptography, Steganoimage.*

INTRODUCTION

Cloud System boosts the information sharing and provides variety of services to the user, according to the studies all the companies share their 80% information with user and 70% information with the supplier by using cloud platform. Now a days cloud services are easily available by requesting network access services which are available with very less cost. whenever user want to share the personal data with third party storage secrecy, authority, authentication, confidentiality are the crucial challenges. While uploading the data sometime physical control can be lost or hackers can hack the data in cloud environment. This can be solved by using combination of steganography and visual cryptography. Steganography is the technique in which data is hidden inside the another file, and cryptography technique refers to secure communication from outside observer.By making use of severalencryption techniques user can store the data on cloud without worrying about the security.

In this paper we are giving the solution for online transaction frauds, phishing by using the steganography and visual cryptography techniques. when customer sharing the transactions details with merchant it can not be directly accessed by the merchant, first it will go to certified authority it will combine the share of customers details and its own details and forms the original information and then it will transfers the fund from customers account to merchants account.

https://doi.org/10.46335/IJIES.2023.8.5.9 e-ISSN: 2456-3463
Vol. 8 , No. 5, 2023, PP. 42-44

II -METHODOLOGY

Steganography

Steganos means Covered or Protected and graphene means writing. This technique in which data hides in such a way that it is difficult to observe. text, images, videos, audios are used by this technique to cover the message. Text steganography uses shifting of words.it is efficient because it requires less memory over others.

Visual Cryptography

Basic idea of this technique is splitting the images in to shares which protects the image and provides security. k out of n(k,n) shares are used by this techniques to form encrypted secret image having shares and forms another image which is meaningless.

Text Steganography

Text steganography uses shifting of words.it is efficient because it requires less memory over others.in proposed method each letter is assigned a number within 0 to 15.different number are assigned by the different frequencies to the alphabets. Number assigned in range (N+0.99)%to (N+0.3)% and (N+0.2)%to (N+0.01)% is same where N is any integer from 1 to 11.it represents frequency of letters in integer form. Following table shows assigned number to alphabet.

Table 1- Assigned number to alphabets

Alphabet	Assigned Number	Alphabet	Assigned Number
A	14	L	10
E	15	M	7
I	13	N	11
O	12	P	7
U	8	Q	0
B	5	R	13
C	9	S	10
D	8	T	11
F	4	V	3

Existing payment method

In existing payment method user has to select the product from site and then add it in to cart and then moved to payment gateway. Online merchants may have their own payment system or they are using third party services. In payment module customer has to submit credit, debit card number, expiry date or CVV number. According to data security standard merchant cannot store private data of the customer. And if merchants want to save, they must have to follow certain security standards.

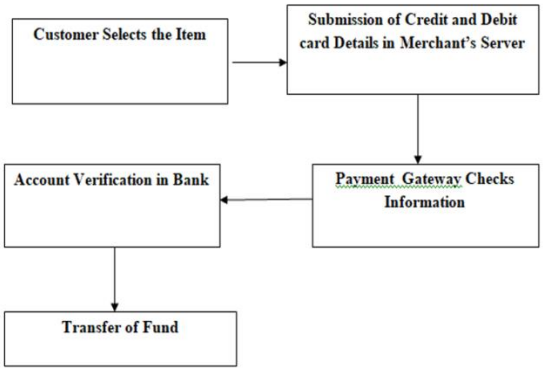

Fig.1-Fig shows existing payment method

Proposed Payment Method

Encoding:

1. In secret message each letter is having ASCII code.
2. Convert ASCII code to 8 bit binary number.
3. Divide 8-bit binary number into 4 bit binary number.
4. Get suitable letter from table with equivalent to 4-bit number.
5. Construct meaningful sentence by using letters obtained as a first letter of suitable words.
6. Avoid articles,pronoun,Preposition,adverb,was/there,is /am/are,has/have/had, Will/shall, would/should in coding process to give flexibility sentence construction.
7. It is not case sensitive.

Decoding:

1. First letter in each message is taken and convert it into 4bit binary number.
2. By combining 4 bit binary number obtain 8 bit binary number.
3. We can get ASCII code from 8 bit binary number.

https://doi.org/10.46335/IJIES.2023.8.5.9 e-ISSN: 2456-3463
Vol. 8 , No. 5, 2023, PP. 42-44

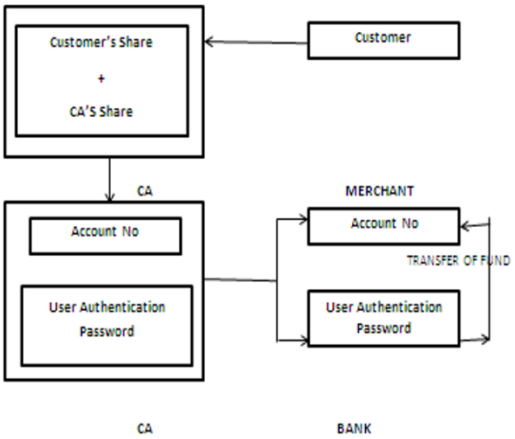

Fig. 2- Fig shows proposed payment method

Solution for the existing payment method is introducing certified authority between the customer and merchant. Customer has to submit very less information to merchant which will verify the payment done by the customer. In proposed method customers password is hide inside the cover text by using text steganography method. Now snapshot of two text is taken and two shares are generated one share is for customer and another is for CA. after receiving one share from customer CA combines the share and get original image.

III -CONCLUSION

While sending the personal or confidential data over cloud there will be any third-party attack occurs. By combining steganography and visual cryptography we are giving secure solution for the data transmission .it secures the customers data at merchant's side which prevents misuse of that data. The method is concerned only with prevention of identity theft and customer data security.

IV -ACKNOWLEDGMENT

I am thankful to the principal and head of the department of computer science from SKN Sinhgad college of Engineering, Korti for providing me sources for this study. I am also thankful to my guide Prof. N.M.Sawant for their valuable guidance on my present study.

REFERENCES

[1] *Souvik Roy; P. Venkateswaran (2017). "Secure Online Payment System using Steganography and Visual Cryptography" Jabalpur University, Kolkata-700032, India.*

[2] *Guangdong Xu(March 2008)."Web Mining Techniques for Recommendation and Personalization",Victoria University, Australia.*

[3] *Bashed Mobster(2007). "Data Mining for Web Personalization,", LCNS, Springer-VerlegBerlin Heidelberg.*

[4] *Dr. R. Krishnamurthy ;K. R. Sabetha,(April 2009). " Identifying User Behavior by Analyzing Web Server Access Log File", International Journal of Computer Science and Network Security.*

[5] *Arya, S.; Silva, M.,(2004)." A methodology for web usage mining and its applications to target group identification", Fuzzy sets and systems, , pp.139-152.*

[6] *R. Kosala;H. Bloc keel(5th of Dec, 2012)," Web mining research: a Survey", SIGKDD Explorations, 2010, 2, pp.1-15. "Log files formats", http://www.w3c.org, Access*

[7] *S. K. Pain, (January 2011). "Web Usage Mining: A Survey on Pattern Extraction from Web Logs", International Journal of Instrumentation, Control & Automation.*

[8] *Min Chen;Jing Chen Shiwen Mao `Privacy Protection and intrusion avoidance for cloudlet based medical data sharing` ,IEEE Transaction on cloud computing.*

[9] *K. Thamizhchelvy; G. Geetha,(2012) "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm." International Conference on Computing Sciences.*

[10] *Anti-Phishing Working Group (APWG),(2013). "PhishingActivityTrendsReport,"http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf*

[11] *AmazonEC2 Instance Types. 16th December (2017).http://aws.amazon.com/ec2/instance types/.*

[12] *J. Chen, T. S; M. W. Cheng, "A New Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on Multimedia Software Engineering.*

[13] *Walter Bender; Daniel Gruel; Morishige Morimoto; A. Lu;"Techniques for Data Hiding," IBM Systems Journal.*