International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

QR based Secure Server Verification by using Encryption Algorithm and Visual Cryptography

Borate Pragati[1], Jambhale Sushma[2], Kad Pranita[3], Kandge Anuja[4]
[1, 2, 3, 4]*Department of computer Engineering, P.K technical campus, ,Pune Unversity,India*

Abstract: ***In today's area of Internet, there are various online attacks are increasing day by day. The most popular attack among them is phishing attack. Phishing attack is an attempt by an individual or a group to gain the personal confidential and sensitive information of user such as passwords, credit card details etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities. So the security us major concern. There is need to build up the system such as "Secure Server Verification by Using Encryption algorithm and Visual Cryptography" to solve the problem of phishing. Visual Cryptography is a secret sharing scheme which uses the technique of sharing the visual information. Visual information (such as printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. This paper gives the information of different techniques used to protect data against the phishing attack and propose the system that can help to maintain the confidentiality of the private data by using visual cryptography and RSA algorithm based on QR code.***

Keywords: Data Mining, Web Application, Portal, Server, GoogleMap, Struts2.0, Microsoft Server R2, E-Commerce

I. INTRODUCTION

In today's internet world, the online transactions are common things. But this online transaction need more security because of various online attacks. The most popular attack is phishing attack in which the user's confidential and sensitive information like credit card details can be hacked by attackers. Phishing attack is known as major attack among all online attacks. Therefore security must be very high which can't be tractable by implementation easiness.

Phishing is a "criminal activity using social engineering techniques". Attacker create a new website which is same as the banking website and attacker send emails to random users. Attacker request to the users to update their password for security and safety. The mail which is sent by attacker contains the fake website. Then attacker use the replica of original website for misguiding users of banking website or government website. After that user fill the sensitive information and attacker take this information to their own illegal website. After taking this confidential information from user, the attacker login to the actual website of bank with the help of id and password which is given by user and then transfer the money from users account to their account. So in this way phishing is the indirect way to steal the money of online user.

To avoid phishing we proposed the system with the visual cryptography algorithm and encryption algorithm which helps to increase the security while doing transaction. We have proposed a new approach named as "QR Code Based Secure Server Verification by Using Encryption Algorithm and Visual Cryptography" to solve the problem of phishing. Here an image based authentication using Visual Cryptography (VC) is used. Visual Cryptography is a secret sharing scheme which owns the technique of sharing the visual information. The QR (image) is getting divided into two shares. The basic idea is that the secret QR is divided into two irregular patterns of images called shares and they can be unrevealed without any complicated cryptographic computation.

II. RELATED WORK

Phishing is a fraud action taken to obtain subtle information like username, password also credit card details, in electronic communication. We can deal with phishing incidence, by taking technical security measures. The evolution of QR code has faster the development of Real time security domain applications. The system uses web application to notify the users through internet. In field of banking security, existing literature mostly relates to algorithm.

III.EXISTING SYSTEM

In the current banking system user can log in to their account using user name and password and for secure login the bank provide the user a unique id to do online banking but for a joint account, there is the same priviledge for log in and access in online banking. It is not mandatory that both users should agree on the transaction in the current system.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

IV. PROPOSED SYSTEM

The proposed methodology is implemented using J2EE (Servelets as a Server side technology). Figure shows the result of creation and stacking of shares. The figure 1 shows the architecture of the proposed system.

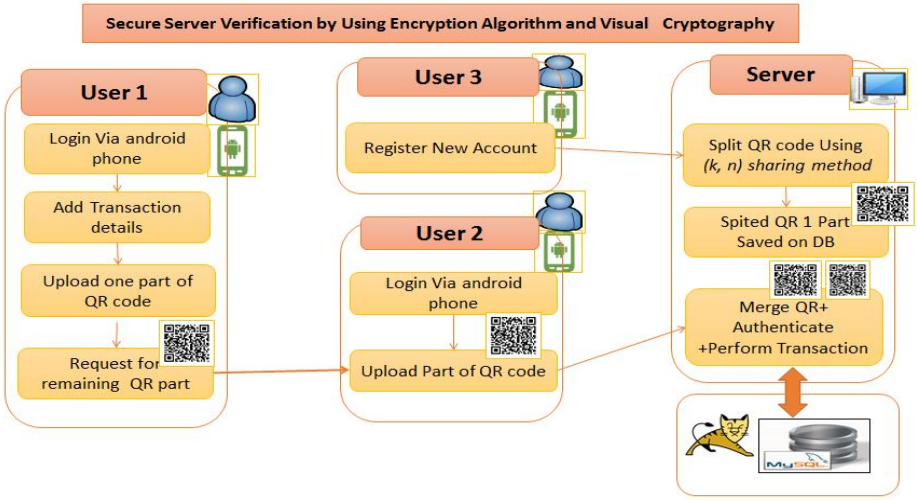

Fig. 1 Architecture

A. Registration Module for Banking

In the registration phase the most important part is the creation of shares from the image where one share is kept with the user and other share can be kept with the server.

B. Verification of Shares using Visual Cryptography

User will upload his/her share and puts his user id and clicks on login button. The share gets uploaded to server and merged with share2 at the server using visual cryptography

If server under test sends some different share then the stacking of shares will create unrecognizable form of image.

1) Visual Cryptography based phishing Website
2) Creation of multiple image shares
3) Forming Original Image on client side

C. Verification of Joint Accounts Transaction

User having joint accounts will upload their shares 1 and puts request to second user for his/her share and second user will upload their share clicks on submit button. These shares gets uploaded to server and merged with share3 at the server using visual cryptography. Merged shared are then compared with the original image to verify the joint account users for fund transfer.

D. Verification of Joint Accounts

If images have to be transferred to each other, it will be transferred in encrypted way using AES and RSA Algorithms. Data will be encrypted using symmetric AES key. Symmetric AES key will be transferred after encrypting with public key of receiver along with the encrypted data.

E. Avoiding Phishing in Banking

Avoid following attacks on the website,

1) Phishers can fake the URL that appears in the address field at the top of user's browser window and redirect him to another web site with the intention of performing fraud.
2) Fraudsters send e-mails with a link to a spoofed website asking you to update or confirm account related information. This is done with the intention of obtaining sensitive account related information like your Internet Banking User ID, Password, PIN, credit card / debit card / bank account number, card verification value (CVV) number, etc.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

V. ALGORITHMS

A. Visual Cryptography

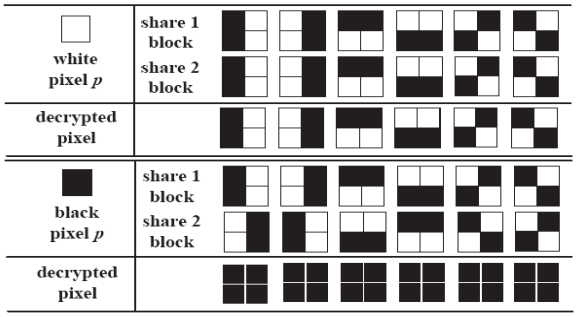

Fig. 2 Visual Cryptography

1) (2,2) Threshold VCS scheme- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

2) (2,n) Threshold VCS scheme-This scheme encrypts the secret image into n shares such that when any two(or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.

3) (n,n) Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants.

4) (k,n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the Threshold, and n, the number of participants.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig. denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.

B. RSA Algorithm

1) *Key Generation:* RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way,

a) Choose two distinct prime numbers p and q. For security purposes, the integer p and integer q should be chosen at random, and should be of similar bit-length.

b) Compute n = pq, n is used as the modulus for both the public and private keys.

c) Compute φ (n) = (p – 1) (q – 1), where φ is Euler's totient function.

d) Choose an integer e such that 1 < e < φ (n) and greatest common divisor of (e, φ (n)) = 1; i.e., e and φ (n) are co-prime. e is released as the public key exponent.e having a short bit-length and small Hamming weight results in more efficient encryption.

e) Determine d as: $D=e^{-1}$ mod(ϕ(n)) d is the multiplicative inverse of e mod φ (n). This is more clearly stated as solve for d given (de) = 1 mod φ(n), d is kept as the private key exponent.

f) By construction, d*e= 1 mod φ(n). The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret. (p, q, and φ(n) must also be kept secret because they can be used to calculate d.)

2) *Encryption:* Sender A does the following: Obtains the recipient B's public key (n, e), 0<=m<n, Represents the plaintext message as a positive integer m such that Computes the cipher text, $C=m^e$(mod n), Sends the cipher text c to B.

3) *Decryption:* Recipient B does the following:- Alice can recover from by using her private key exponent via computing . Extracts the plaintext from the integer representative m.

C. AES Algorithm

AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The numbers of cycles of repetition are as follows:

1) 10 cycles of repetition for 128-bit keys
2) 12 cycles of repetition for 192-bit keys
3) 14 cycles of repetition for 256-bit keys

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

VI.OUTCOMES

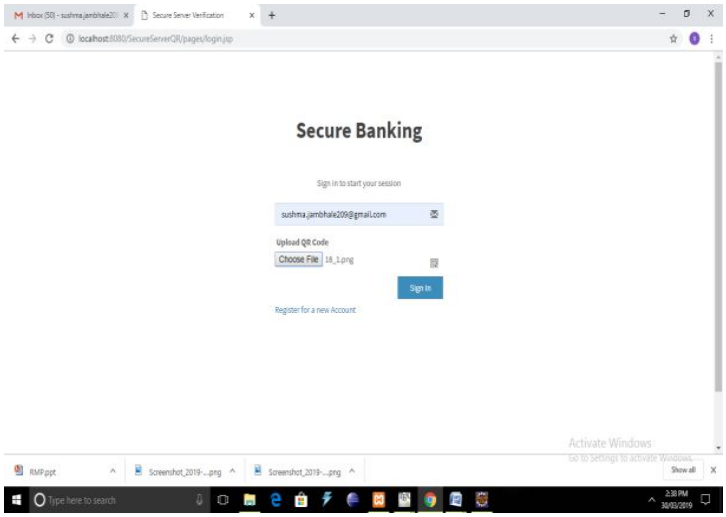

Fig. 3 User Login Page

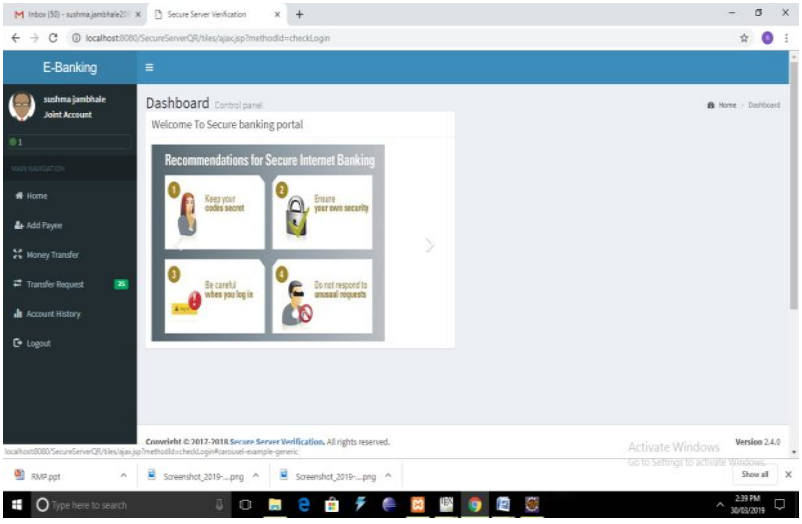

Fig. 4 User's Dashboard

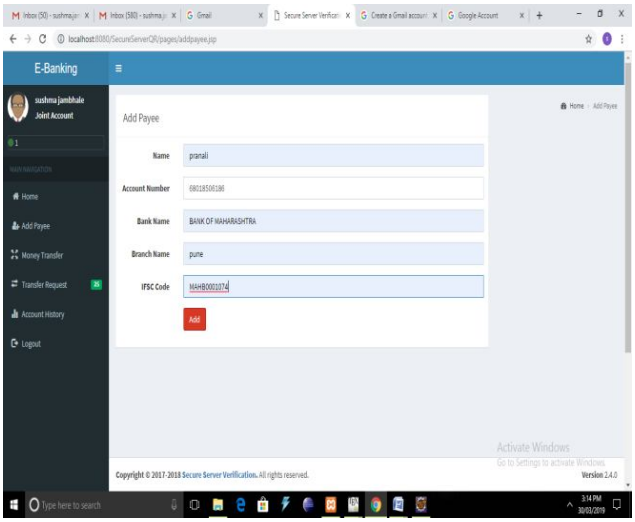

Fig. 5 Add Payee details

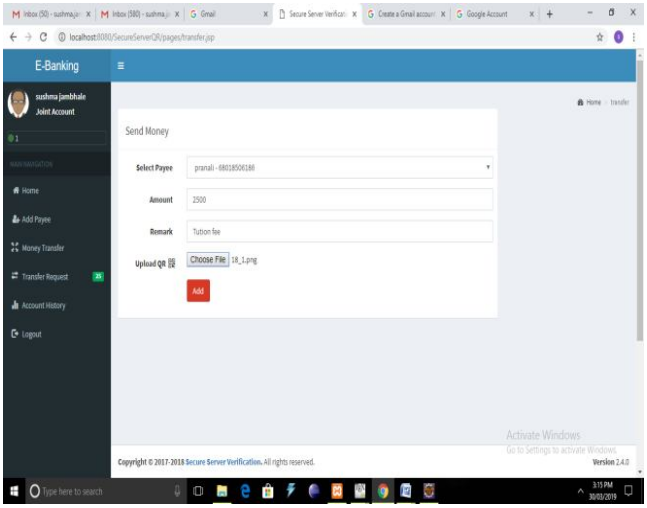

Fig. 6 Add Money Transfer details

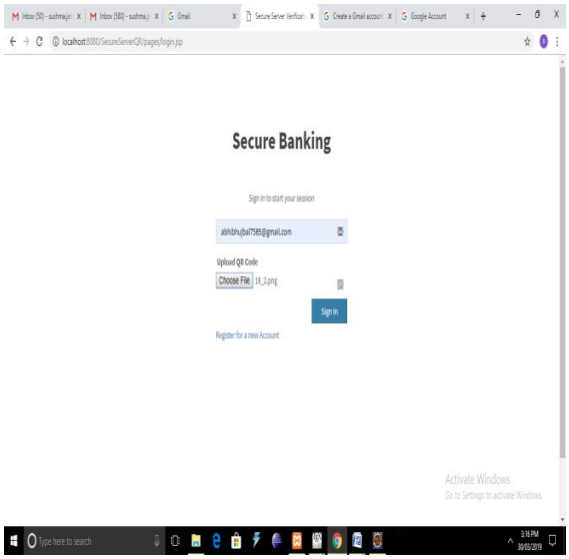

Fig. 7 Login of second User

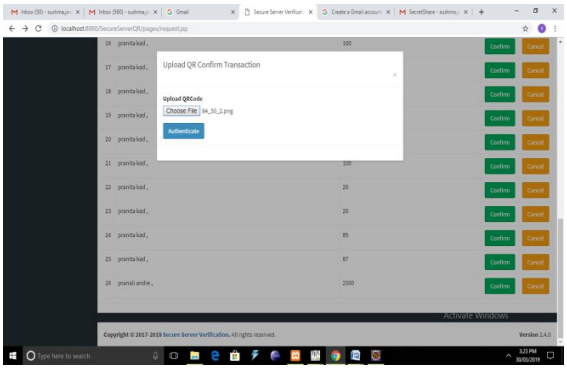

Fig. 8 Give permission to transfer money

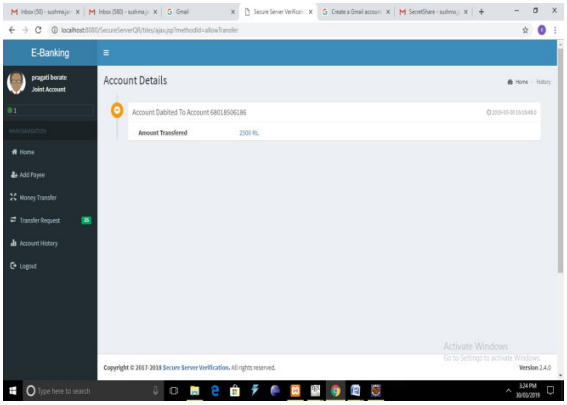

Fig. 9 Transaction successful

VII. CONCLUSIONS

In the scope of visual cryptography various researcher have implemented different technology who's survey is mentioned in our paper. With the reference concluded from various reviews taken from papers we came to know that not a single present system gives 100 % of accuracy while protecting data being phished by phishing attack. That is motive of obtaining subtle account related details like password, PIN, Internet Banking User Id, credit card / debit card manipulations by the unauthorized users. We here defined a system which can prevent the data stealing through phishing attacks. And as well provide efficient authentication between joint account holders to use their joint account. The system provides security for banking system by providing the authentication which can be completely trusted. And, which can protect us against phishing attack.

REFERENCES

[1] A. Shami r, "How To Share a Secret", Commun. ACM, vol. 22, pp. 612-613, 1979.

[2] G. R. Blakley, "Safe guarding cryptographic keys", in Proceedings of the 1979 AFIPS National Computer Conference, 1979, pp. 313-317.

[3] D.S. Wang, Z. W. Ye, and X.B. Li , "How to Collaborate bet ween Threshold Schemes", arXiv:1305.1146v1, pp. 1-14.

[4] M. Naor and A. Shamir, "Visual Cryptography", Adv. Cryptogr., pp. 1-12, 1995.

[5] C.N. Yang, "New visual secret sharing schemes using probabilistic method", Pattern Recognit. Lett., vol. 25, no. 4, pp. 481-494, 2004.

[6] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes", Comput. J., vol. 49, no. 1, pp. 97-107, 2006.

[7] D.S. Wang, F. Yi, and X.B. Li , "Probabilistic visual secret sharing schemes for grey-scale images and color images", Inf. Sci. (Ny)., vol. 181, no. 11, pp. 2189-2208, 2011.

[8] Divya James,Mintu Philip,"A Novel Anti Phishing framework based on Visual Cryptography",2012 IEEE.

[9] Sozan Abdulla "New Visual Cryptography Algorithm For Colored Image", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 4, APRIL 2010, ISSN 2151-9617.

[10] Shreya Zarkar, Sayali vaidya, Arifa Tadvi, Tanashree Chavan, Prof. Achal Bharambe "Image Based Authentication Using Visual Cryptography and Encryption Algorithm "(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1692-169.