iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 Issue: III Month of publication: March 2015

DOI:

www.ijraset.com Volume 3 Issue III, March 2015
IC Value: 13.98 ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Anti-Phishing Framework Using QR Code Validation Scheme Based On Visual Cryptography

Sneha Mali[1], Sumita Tanpure[2], Komal Kumkar[3], Swapnali Patil[4], Prof. S.A. Darade[5]
[1,2,3,4,5] *Sinhgad Institute of Technology and Science, Narhe, Pune-410041,India*

Abstract-Due to new innovations and ideas in internet technologies many web applications, mainly in e-commerce application; online transactions have become most popular feature for these domains. Now-a-days as use of internet for transactions has grown, the threat of security over internet has also grown. The threat concerned with security includes many attacks like Denial of Service, E-mail spoofing, phishing, viruses and worms, etc. One of the most popular and familiar attack used by hackers is phishing and is carried out by hackers with an intention to gain confidential data, credential information like password, credit/debit card number. Therefore there is need to create a new methodology to prevent from such type of attacks. Hackers use this attack in many fields, including mainly in e-commerce and banking domains and it has been recorded in history. Here, in this paper we describe a methodology for phishing detection and prevention which can be used to detect the phishing website. It is based on the Anti-Phishing framework using QR Code validation scheme based on visual cryptography. Using this framework, user can verify whether the website is fake or real and prevents user from entering password and other confidential information to the phishing websites.

Keywords— Phishing, Shares, Visual Cryptography, Encryption, Decryption, QR Code

I. INTRODUCTION

Phishing is similar to fishing where a hacker instead of trying to catch fish, he attempts to steal your personal information like passwords. Phishing is an attack carried out by an individual person or a group of people with an intension to steal confidential data like credit card details, passwords, etc. To attempt this attack, Hackers creates a fake website which is made to appear similar to original website. Phishing is popular and commonly used among hackers, which has lead challenges to developers to build new application system considering the security and prevent it with the help of new innovative ideas and technologies. As system provide security itself, the design and technology of middleware is advanced and improved rapidly, so detection is difficult. As a result, it is impossible to detect the computer connected over internet is secure or not. Phishing scams is becoming a problem for daily e-commerce users and banking users as they do daily online transaction. Therefore, there is need of high level security. In times there have been many methodologies to detect phishing but somehow they have problems like complication, time constraints, less security. So here is the solution for above problem, introducing a new enhanced method to detect phishing and is a safe and secure way to prevent against phishing, named as “Anti-Phishing framework using QR Code validation scheme based on visual cryptography”. As the name suggest, in this methodology, a website is cross verified whether it is a genuine or phishing website. Here we use the concept of visual cryptography method and one time password. Here, One Time Password (OTP) is converted to QR Code and Visual Cryptography (VC) is applied to divide the QR Code images into two shares and in order to reveal original QR Code image the shares are combined again.

A. Visual Cryptography

Cryptography is one of the best and popular techniques used to protect and enhance the security of data. It is an art of sending and receiving messages on which encryption is performed by sender and decryption is performed by receiver only. These activities are carried out by sender and receiver in such a way that only recipient is able to read the message after decryption and is carried out using various mathematical algorithms.

Naor and Shamir [3] introduced Visual Cryptography scheme (VCS) which is simple and secure as it allows without cryptographic computations to share secretly images. A brief survey is presented to the work related in the area of visual cryptography. Shamir [4] and Blakley [5] introduced Visual cryptography schemes independently with an intention to prevent cryptographic keys from loss.

These schemes have widely application in many different areas and are used to construct several types of cryptographic protocols. Borchert suggested a segment-based visual cryptography technique. This technique can only be used to encrypt the messages containing symbols, numbers like bank account number, amount etc. Wei-Qi Yan proposed VCS which is applied only for printed text or image. The research work done in VC previously has focused on improving pixel expansion and contrast. The research work suggests that all participants who hold the shares should not present false or fake shares during while recovering secret image and should be honest. Thus the image created by stacking of shares is considered as the real secrete image. Yan, Horng and Hu introduced cheating prevention methodologies as this may not be true always. But, in all these cases, facility of authentication testing is not provided in these methodologies.

VCS is a cryptographic technique which performs encryption of visible information and uses human visual system to perform decryption. This can be achieved by using any of the following access structure schemes:

1) (2, 2)- Threshold VCS Scheme: This threshold scheme takes a secret message and encrypts it by dividing one share into two different shares that reveal the secret image when they are combined is simplest scheme.

2) (n, n) -Threshold VCS Scheme: This scheme encrypts the secret image in n shares and when this all n shares are combined the secrete image can be revealed.

3) (k, n) Threshold VCS Scheme: This scheme encrypts the secret image and divides the image to n shares and when combined with any group of at least k shares, the secret image can be revealed.

B. QR Code

QR code stands for Quick Response Code and it is like two-dimensional barcode. This barcode can contain information about any item to which it is attached and is machine-readable optical label. Now-a-days, the QR Code system has become popular due to its feature like greater storage capacity and readability. A QR code on white background consists of black arranged in a square grid. This can be done by reading using an imaging device such as a camera. Here, in the proposed system, QR Code is generated from One Time Password which is nothing but string generated and is converted to QR Code. After performing Visual Cryptography, QR Code is divided into shares and combined again to reveal the original QR Code image. This QR Code is scanned against camera to get the password, which will be entered by user.

II. CURRENT METHODOLOGY

In the current scenario, anti-phishing framework works as shown in the figure 2.1. [2] This framework is an enhancement in previously proposed system defined in Anti-Phishing Framework Based on Visual Cryptography. [1]

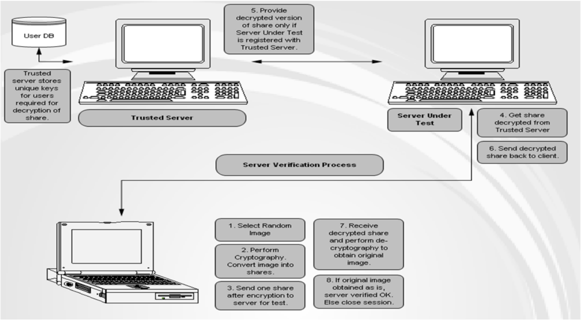

User DB
Trusted server stores unique keys for users required for decryption of share.
Trusted Server
5. Provide decrypted version of share only if Server Under Test is registered with Trusted Server.
Server Under Test
4. Get share decrypted from Trusted Server
6. Send decrypted share back to client.
Server Verification Process
1. Select Random Image
2. Perform Cryptography. Convert image into shares.
3. Send one share after encryption to server for test.
7. Receive decrypted share and perform de-cryptography to obtain original image.
8. If original image obtained as is, server verified OK. Else close session.

Fig 2.1 Current Scenario

In this methodology first users are registered with the trusted server. At the time of registration, the admin generates unique key and this unique key is stored within the database of trusted server. Once the user is registered he logins through client application using username and password. In the system for a particular time, user selects random image to verify the server under verification. User performs cryptography using client application on that image, to convert image into shares. One of the encrypted shares is send to server under verification. For decryption, the server under verification forwards the share along with its id and password to get share decrypted from trusted server. The trusted server performs decryption using the unique key stored within it & provides decrypted share to the only server which is registered within trusted server. After receiving the share, the server under verification sends it to client. The client performs de-cryptography to obtain original image. After combining the image, if the original image is obtained then the server under verification is non-phishing otherwise it is detected as phishing site. The original image can be obtained if and only if both the user and server under verification are registered, if not then the system generates wrong image. This methodology has problems like the user performs most of all work i.e, selecting random image, performing cryptography and decryptography. Also the security provided is less. User work is made complicated.

III. PROPOSED METHODOLOGY

To overcome the above problems and for better phishing detection and prevention, here we propose a new advance and enhanced methodology, based on the Anti-Phishing framework using QR Code Image validation scheme based on Visual Cryptography. The figure 3.1 below shows the framework that we are implementing.

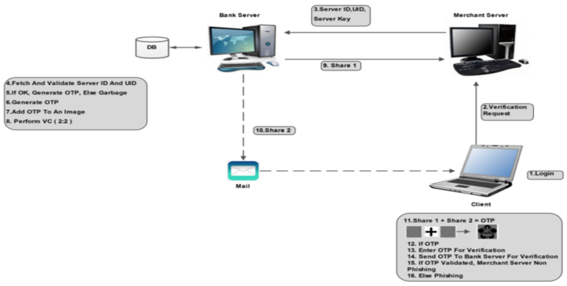

Bank Server
3.Server ID,UID, Server Key
Merchant Server
DB
9. Share 1
4.Fetch And Validate Server ID And UID
5.If OK, Generate OTP, Else Garbage
6.Generate OTP
7.Add OTP To An Image
8. Perform VC (2:2)
2.Verification Request
10.Share 2
Mail
1.Login
Client
11.Share 1 + Share 2 = OTP
12. If OTP
13. Enter OTP For Verification
14. Send OTP To Bank Server For Verification
15. If OTP Validated, Merchant Server Non Phishing
16. Else Phishing

Fig. 3.1 Framework

In proposed methodology, the users and merchant server are registered on bank server i.e trusted server. The user needs to login with User Id (UID) and Password provided during registration. These details are sent to merchant server. The merchant server will add its details like Server ID and password and sent it to Bank server for authentication. Bank Server fetches details and carries out authentication process on the details received. If process results in success i.e, both are authenticated user, then bank server proceeds toward further process. Bank server will generate OTP (One Time Password). This OTP is merged to QR code image and Visual Cryptography is performed. While performing Visual Cryptography, Grey Scaling and Thresh holding algorithms are carried out. Grey Scaling results into image in which the value of each pixel is a single sample, the intensity information is carried. Thresh holding is applied for segmentation where a grey scale image is used to create binary images. After this the share generation algorithm is performed where two shares are generated. Share 1 will be send to merchant server and another to user via mail. These two shares are combined where user enters it share on the client application where merchant server's share is already entered, and if both shares are matched then only OTP is generated after scanning the QR Code against camera. The user needs to enter the OTP and bank server checks for validation in session time provided. If validation process is successes then the merchant Server is non phishing else it is detected as phishing. If session time expires OTP is generated once again and further process is carried out.

With respect to phishing attacks, this framework supports for complete security for web application. It helps to prevent confidential information like password and other information from the phishing websites. The proposed system can easily handle by user as there are no complications more. User tasks are reduced, hence making the system simple for the use.

IV. CONCLUSION

Currently phishing attacks are so popular and commonly used as it retrieves users' confidential data. This information can be used by the attackers or hackers to carry out phishing attack and is indirectly part of the attack. Phishing websites can be easily detected and prevented using our proposed "Anti-Phishing framework using QR Code validation scheme based on visual cryptography". The propose methodology can be used to easily identify the website is genuine or phishing website and it is more secure as One Time Password is converted to QR code and then encryption and Decryption is performed to generate the shares. Since after decryption the OTP is needed to be provided in particular session time and are not stored, they could not be stolen and hence it is more secure. Every time, when online transactions are carried out by user new password is generated for security, hence user can safely use the system.

REFERENCES

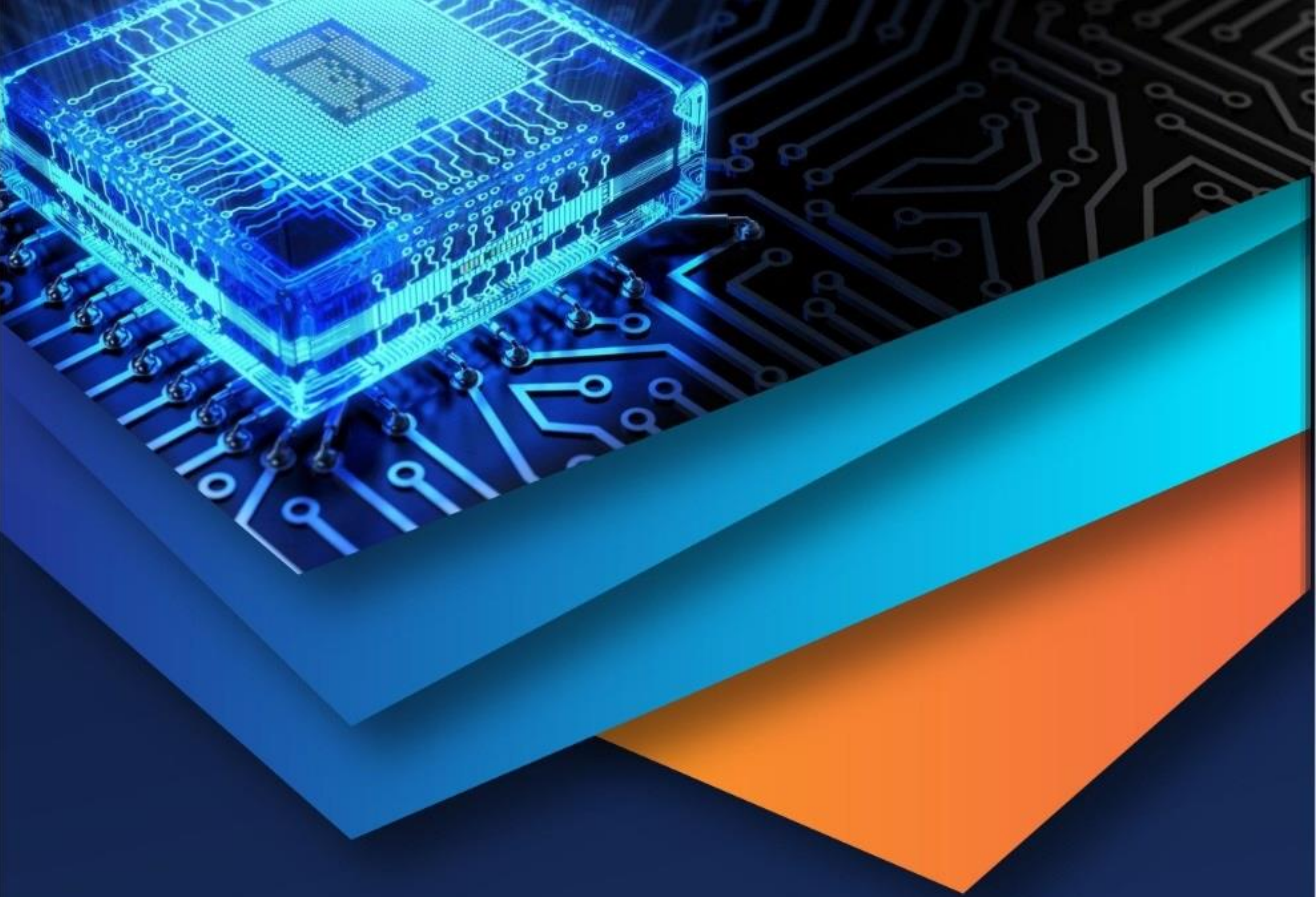
[1] "A Novel Anti Phishing framework based on Visual Cryptography", in Proceedings of Power, Signals, Controls and Computation (EPSCICON), Divya James.; Mintu Philip, 2012.

[2] "Visual cryptography," in Proc. EUROCRYPT,1994, M. Naor and A. Shamir.

[3] "An Enhanced Anti-Phishing Framework Based on Visual Cryptography", International Journal of Emerging Research in Management &Technology, Gaurav Palande, Shekhar Jadhav, Ashutosh Malwade, Vishal Divekar, Prof. S. Baj, ISSN: 2278-9359 (Volume-3, Issue-3)

[4] "How to Share a Secret",. Communication ACM, A. Shamir,.

[5] "Safeguarding Cryptographic Keys",.Proceedings of AFIPS Conference, G. R. Blakley.



10.22214/IJRASET

INDEX COPERNICUS 45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429