Implementing Securing online banking using Visual Cryptography schemes using QRCode

Najan Parimal Vishnu, Thakare Mayuri Kishor, Amjad Raza, Nayal Gayatri J S
(Students, Dept. of Computer Engineering, Sinhgad Academy of Engineering, Pune, Maharashtra, India,

M.E.SANAP
Assistant Professor, Dept. of Computer Engineering,
Sinhgad Academy of
Engineering, Pune, Maharashtra, India.

Abstract: ***-Nowadays many people are using online financial transactions. This transaction needs to be secure. A rapid growth in E-Commerce market is seen in recent time throughout the world. With the ever-increasing use of online shopping, Debit or Credit card fraud and personal information security are major concerns for customers, merchants and banks specifically in the case of CNP (Card Not Present). There are various attacks present behind this. Phishing is one type of attack. For detecting this attack, various anti-phishing mechanisms are used. In phishing process, suppose cheater sends out thousands of phishing emails with a link to the fake website. Victims click on links in email believing it is legitimate. They enter personal information on that fake website. Fraudsters collect the stolen data and login into correct website. This is an overall process of phishing.We propose a new scheme for online fraud transaction prevention using extended visual cryptography and QR codes. This scheme uses extended visual cryptography for share generation. One time password is used for phishing website detection. Extended visual cryptography is used for converting the QR code into two shares. The system provides security for online users and detecting the phishing websites.***

I. INTRODUCTION

In online transactions various types of attacks can take place, phishing is identified as a major security threat, and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective. Today, most of the applications are only as secure as their parent system. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet is completely secure or not. Phishing has also become a problem for online transactions. Thus, security in such cases should be very high which cannot be tractable by implementation easiness. Phishing can be defined as it is a criminal activity using social engineering techniques.

Security is very important term during an online transaction. Various security attacks present behind this online transaction. So, we propose the new idea in this paper for providing the security. In phishing process, suppose cheater sends out thousands of phishing emails with a link to the fake website.

Following figure shows phishing process victim clicks on links in email believing it is legitimate. He enters personal information on that fake website. Fraudster collects the data entered by victim and login into correct website. This is an overall process of phishing.

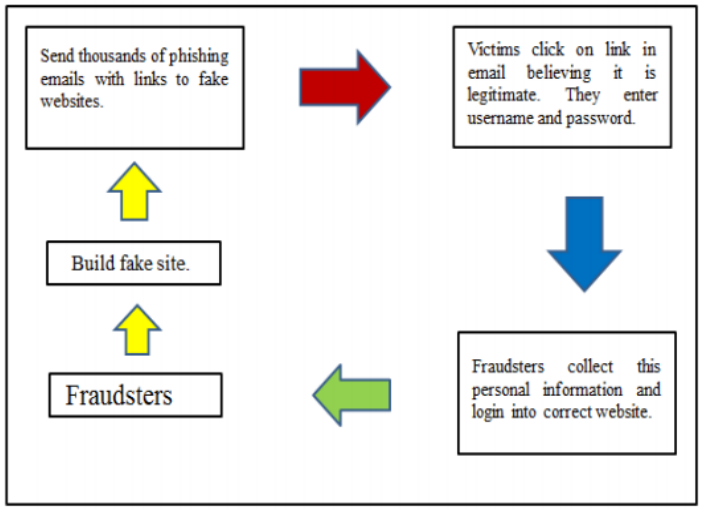

Figure: - Phishing Process

Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?

The answer to the above is that 462 locks are needed and also 252 keys per scientist. Obviously this is not practical. Furthermore, consider a more realistic scenario: A company that develops software signs its software deliverable with its RSA secret key in order to verify its authenticity. A possible approach would be to give a copy of the key to all of the senior developers and any of them can use that to sign each release. However, that's easy to abuse. On the other hand, multiple keys can be issued and distributed to developers and each release would require all of them to sign it. This provides powerful safety about the authenticity of the software but it is very inconvenient.

Putting all this into the context of SSSS a secret key S can be split into N parts (and distributed to N senior developers/scientists) such that any k out of N are required reconstructing the secret key. Immediately, the inconvenience is eliminated and even more, there is room for drop outs (i.e. senior developer leaves company). Such a fascinating scheme. Nothing less expected from the co-inventor of RSA.

II. EXISTING SYSTEM

Some banks generate and dispatch OTPs to the customer's mobile phone via SMS or mobile Transaction Authorization Numbers (mTANs). In some countries, banks still use hard copy methods to deliver OTPs, usually on paper or in the form of a plastic scratch card. All OTP systems share the same flaws and vulnerabilities. First, they are all symmetric because the bank has access to the same secrets as its customer (and the mobile carrier does too, in the case of SMS transmission). Secondly, OTP systems all remain reliant on browser-based communications back to the bank. This means that if a phishing site mimics the bank's online banking or the browser is otherwise compromised, the customer's credentials and the OTP can be harvested by fraudsters and immediately used to gain access to accounts and authenticate fraudulent transactions.

A hacker intercepts communications between a bank and its customer. The legitimate parties are unaware of the hacker's presence, enabling the fraudster to act as a proxy – the "man in the middle." In phishing, an unauthorized user copies the user's ID, password and OTP, and immediately uses them.

III. LITERATURE SURVEY

This section consists of the work that has been already done on this system by various researchers using different methodologies and algorithms.

METHOD: - Visual Cryptography and OTP.

DESCRIPTION:-The malicious website detection using visual cryptography and OTP is proposed. It is used to solve the problem of phishing. In this approach, image based validation using visual cryptography is implemented with the grouping of OTP. The use of visual cryptography is open to preserve the secrecy of an image captcha by dividing the original image captcha into two shares. The original image is gained at the user end only when both the user and the server are registered with the trusted server. Using this, website cross validates its identity and proves that it is an honest website before the end users.

XingxingJia et al. designed A (k, n)-conventional visual cryptography (VC) method to share one secret and each participant takes one share. Collaborative visual cryptography (CVC) schemes into the multiple secrets VC scheme with a general access structure. The structure of the basis matrices in CVC method in between two VC schemes is formulated into an integer linear programming problem that minimizes the pixel expansion under the corresponding security and contrast constraints. In addition, the collaboration among more VC schemes is constructed.

METHOD: - VISUAL CRYPTOGRAPHY USING THE QR CODE

DESCRIPTION:-Image-based verification using visual cryptography is proposed. Visual cryptography is use to transform the QR code into two shares and both these shares transmitted separately. This methodology was implemented image based authentication using visual cryptography. Using this method, the user can determine wh ether the site is safe or unsafe to carry out his transaction.

ADVANTAGE: - This system proves that QR Code method is more efficient and secured.

TanashreeChavan et al. demonstrate an Anti-phishing structure based on visual cryptography and RSA algorithm. An image-based authentication using Visual Cryptography (VC) and the encryption algorithm (RSA) is used to avoid phishing.

This method of image authentication gives 100% result for image size less than 2.5MB. Consequently, security of image can be attained by visual cryptography and RSA algorithm.

METHOD: - Visual cryptography using EVC and QR code

DESCRIPTION: -In this paper new scheme for providing security during an online transaction for online frauds detection using Extended Visual Cryptography (EVC) and QR code. By using this technique, we provide better security to people. In proposed system user first registered on the website. The client sends ID and password to bank server for verification. If it is valid then generate One Time Password (OTP) and apply EVC for shares generation. Bank server sends one share to the client and one share to the server. At the time of reconstruction, two shares are combined to reveal the original OTP. Then the client sends this OTP to bank server for verification.

A. Shami r et al. shows how to divide data D into n pieces in such a way that D is easily reconstruct able from any k pieces, but even complete knowledge of k - 1 pieces reveals absolutely no information about D. This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches ex- pose all but one of the remaining pieces.

METHOD: - Hash-based scheme

DESCRIPTION: -For user authentication, we have to proceed through verification of the ID and password to the system verification of password system uses a hash-based password scheme that converts the original password into hash-value by famed function. The advantages this system without difficulty and computational velocity of a process is fast because a type of hash-based scheme is fundamentally based on text utilizing popular hash function such as MD5, SHA256. Suppose that someone writes password "1qaz2wsx" in a system. If an attacker is aware of the hash value "1c63129ae9db9c60c3e8aa94d3e00495", the value can be sufficiently cracked simply by the free crack site. If the attacker doesn't know any information about hash function, he or she can easily guess which kind of hash function is used in the system. As the result, the attacker can cause damage to the system.

METHOD:-**Steganography scheme**

KEY CONCEPT:-For hiding a message we are using steganography. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. For hiding data in steganography using text, video, and image cover the message.

DESCRIPTION: - The text message can be hidden by shifting word and line, in open +spaces, in word sequence of a text steganography. Properties of a sentence such as a number of words, number of characters, the number of vowels, the position of vowels in a word are also used to hide a secret message. The advantage of text steganography over other steganography techniques is its smaller memory space requirement and simpler communication. Visual Cryptography (VC), proposed by Naor, is 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.

IV. PROPOSED WORK

.Proposed System

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

1. **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.

2. **Verification of Shares or Login 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

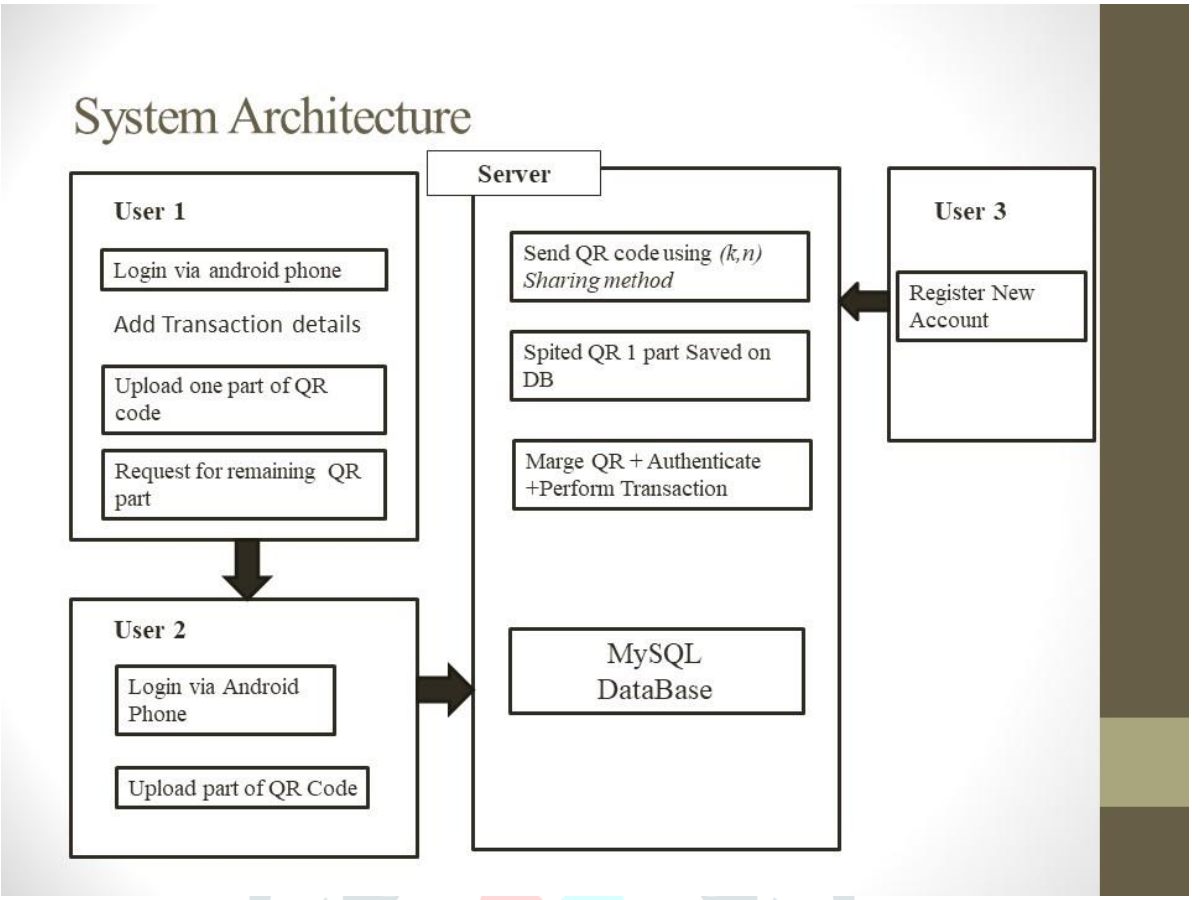

Figure: - System Architecture

3. **Verification of Joint Accounts**

   User having joint accounts will upload their shares 1 by 1 and puts their user id and clicks on login 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.

4. **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.

5. **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.

Advantages of Proposed System

1. To prevent user account details from phishing attack.
2. To perform authentication of both users of joint account to avoid anonymous use of account by single user.

V. ALGORITHMS USED

ALGORITHM 1:- K-N Sharing method

More particularly Shamir Secret Sharing Scheme (SSSS) ***enables to split a secret S in n parts such that with any k-out-of-n pieces you can reconstruct the original secret S, but with any k-1 pieces no information is exposed about S. That is conventionally called a (n, k) threshold scheme.***

At first this may seem counterproductive in the context of secure data transmission because if there is a secure way of distributing a secret S amongst participants what is the point of using this scheme. The original purpose of the scheme is to enhance practicality and convenience when multiple parties are required to perform an authorised action. For instance consider the following problem statement from

Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?

The answer to the above is that 462 locks are needed and also 252 keys per scientist. Obviously this is not practical. Furthermore, consider a more realistic scenario: A company that develops software signs its software deliverable with its RSA secret key in order to verify its authenticity. A possible approach would be to give a copy of the key to all of the senior developers and any of them can use that to sign each release. However, that's easy to abuse. On the other hand, multiple keys can be issued and distributed to developers and each release would require all of them to sign it. This provides powerful safety about the authenticity of the software but it is very inconvenient.

Putting all this into the context of SSSS a secret key S can be split into N parts (and distributed to N senior developers/scientists) such that any k out of N are required to reconstruct the secret key. Immediately, the inconvenience is eliminated and even more, there is room for drop outs (i.e. senior developer leaves company). Such a fascinating scheme. Nothing less expected from the co-inventor of RSA.

K-Shares generation process(Encryption Phase).

Given the above, let's go ahead and try to work how the scheme works with numeric values. Let us say that our secret message is the text "SeCrEt" converting this to hex we have 0x536543724574 and continuously to decimal this is equivalent to 91694388364660. Thus S = 91694388364660, also let the N = 5 and k =3. That is, we will split the text "SeCrEt" into 5 pieces and with any 3 of them we can reconstruct the text.

First, we sample k-1 random numbers $\{a_1, a_2 \ldots, a_{(k-1)}\}$ from a finite field of size p where:

$$p \in \mathbb{P} : p > S, p > n$$

such that $a_i < p$ and $a_0 = S$. Then those are used to generate the polynomial:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1}$$

Back to our example we choose p = 91994388364979. Then we generate random numbers:

$$a_1 = 5481390490034$$
$$a_2 = 4103884901909$$

And as a result the following polynomial is generated:

$$f(x) = 91694388364660 + 5481390490034x + 4103884901909x^2$$

The next step is to construct the N pieces that are distributed to the participants. Each piece is simply a point on the polynomial just defined. Each point D can be calculated in an iterative manner:

$$D_{x-1} = (x, f(x) \ mod \ p))$$
$$where \ \ x = 1, 2, ..., N)]))$$

In our case we need 5 points so we calculate them as follows:

$$D_0 = (1, f(1) \mod p) = (1, 9285275391624)$$
$$D_1 = (2, f(2) \mod p) = (2, 27078320587385)$$
$$D_2 = (3, f(3) \mod p) = (3, 53079135586964)$$
$$D_3 = (4, f(4) \mod p) = (4, 87287720390361)$$
$$D_4 = (5, f(5) \mod p) = (5, 37709686632597)$$

These are then distributed to the participants of the scheme.

K-Shares Merging process (Decryption Phase)

In order to reconstruct the original secret from any k-out-of-n parts, we need to recreate the polynomial that we defined in the beginning. This can be achieved with the Lagrange Polynomial Interpolation. This is simply a formula named after the Italian mathematician Joseph Louis Lagrange for interpolating a polynomial of a degree less than n that passes through n points.

Initially, the Lagrange Basis Polynomials need to be calculated. The formula for the basis polynomials is defined as follows:

$$\ell_j(x) := \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m} = \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_k)}{(x_j - x_k)},$$

Then, given n points, the interpolated polynomial is a linear combination of the above basis polynomials as shown below:

$$f(x) = \sum_{j=0}^{n-1} y_j l_j(x)$$

Applying this to our example we randomly select 3 out of the 5 points we derived above:

(x0, y0)=(1, 9285275391624), (x1, y1)=(2, 27078320587385), (x2, y2)=(4, 87287720390361)

Then the basis polynomials become:

$$l_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{1}{3}(x - 2)(x - 4)$$
$$l_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = -\frac{1}{2}(x - 1)(x - 4)$$
$$l_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{1}{6}(x - 1)(x - 2)$$

And the interpolated polynomial is derived from:

$$f(x) = \sum_{j=0}^{2} y_j \cdot l_j(x)$$

Therefore:

$$f(x) = \frac{9285275391624}{3}(x - 2)(x - 4) - \frac{27078320587385}{2}(x - 1)(x - 4) + \frac{87287720390361}{6}(x - 1)(x - 2))$$
$$f(x) = 4103884901909x^2 + 5481390490034x - 300000000319 \ (mod\ p)$$
$$f(x) = 4103884901909x^2 + 5481390490034x + 91694388364660 \ (mod\ p)$$

Note that since we are working over the Finite Field $Z_{91994388364979}$ the negative -300000000319 can be changed to +91694388364660. And guess what… if this number looks familiar you are right! This is our secret.

ALGORITHM 2:- *RSA* Algorithm

In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric.

Algorithm: - It provides a method to assure the confidentiality, integrity, authenticity, and non-repudiation of electronic communications and data storage.

TABLE I. RSA ALGORITHM [1]

Step 1	• Two prime numbers are selected as **p *and q*.** • For security purposes, integer's ***p* and *q*** should be chosen at random bases and should be similar in magnitude but it should be 'differ in length by a few digits to make factoring harder.
Step 2	• **n = pq,** which is the modulus of both the keys. • ***n*** is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
Step 3	• Calculate totient, **totient = (p-1)(q-1)**
Step 4	• Choose e such that **e > 1** and coprime to totient which means **gcd (e, totient)** must be equal to **1, e** is the **public key.**
Step 5	• Choose d such that it satisfies the equation; **de = 1 + k (totient)**, **d** is the private key not known to everyone.
Step 6	• Cipher text is calculated using the equation; **c = m^emod n** Where **m** is the **message**.
Step 7	• With the help of **c and d** we decrypt message using equation ; **m = c^dmod n**. Where **d** is the **private key.**

ALGORITHM 3:- AES Algorithm

The Advanced Encryption Standard (AES) algorithm is one of the block cipher encryption algorithm.

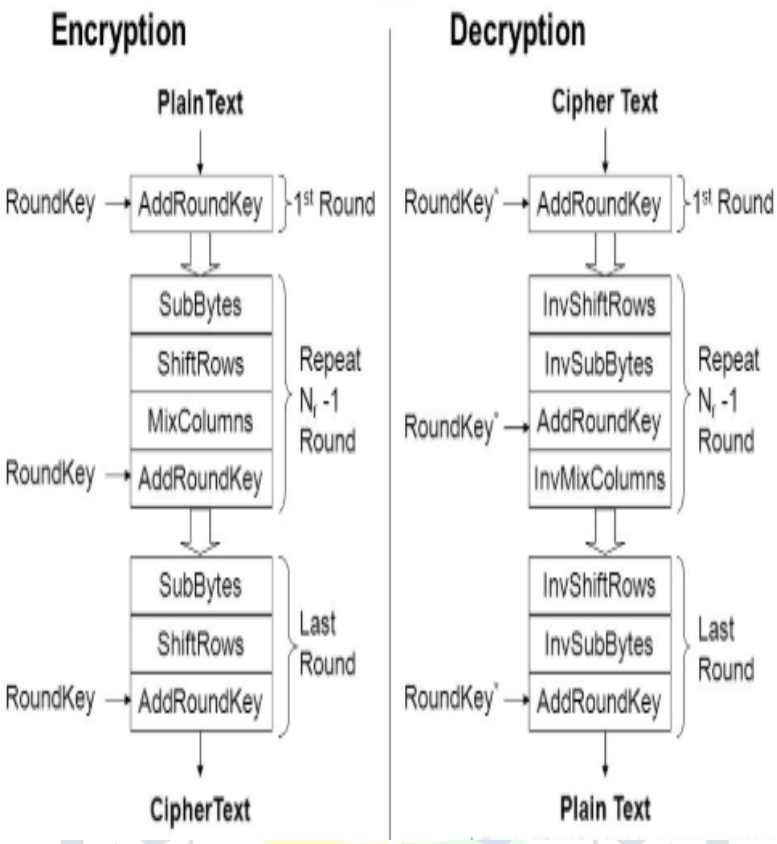

Figure: - AES Algorithm Stepwise.

VI. RESULT AND ANALYSIS

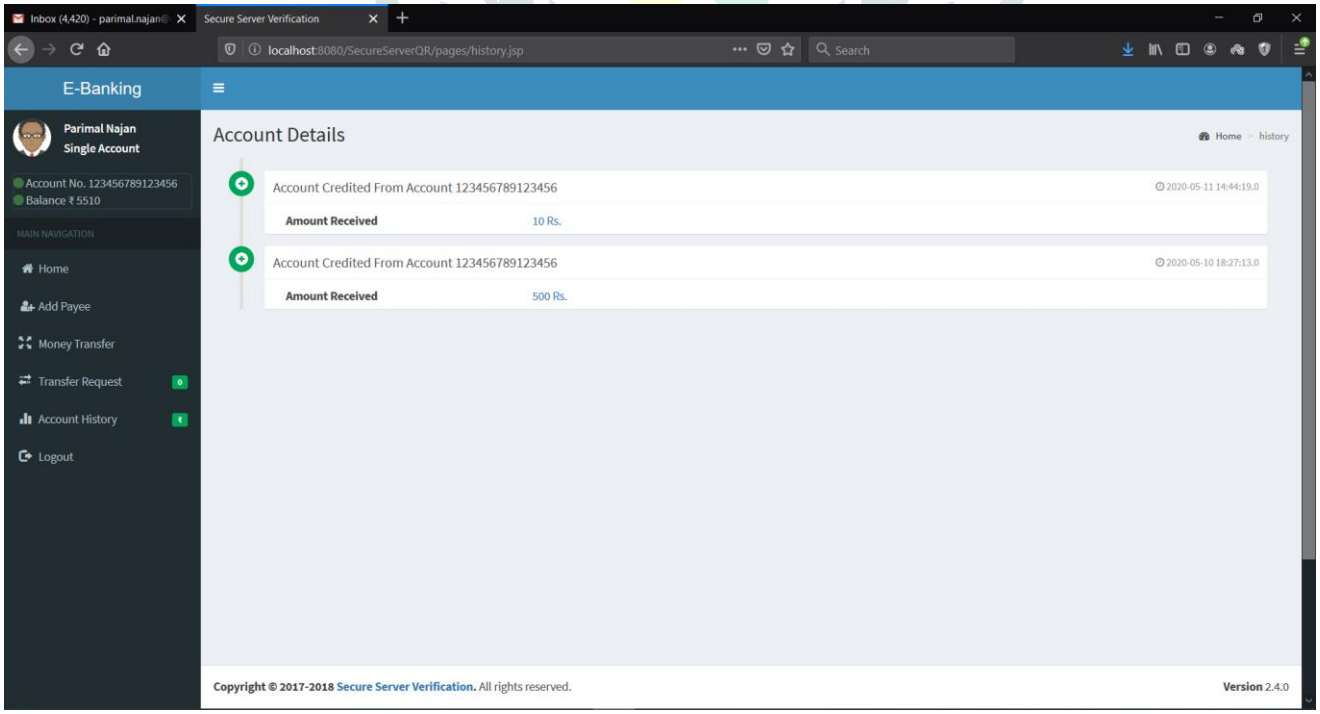

Figure:- Account Details

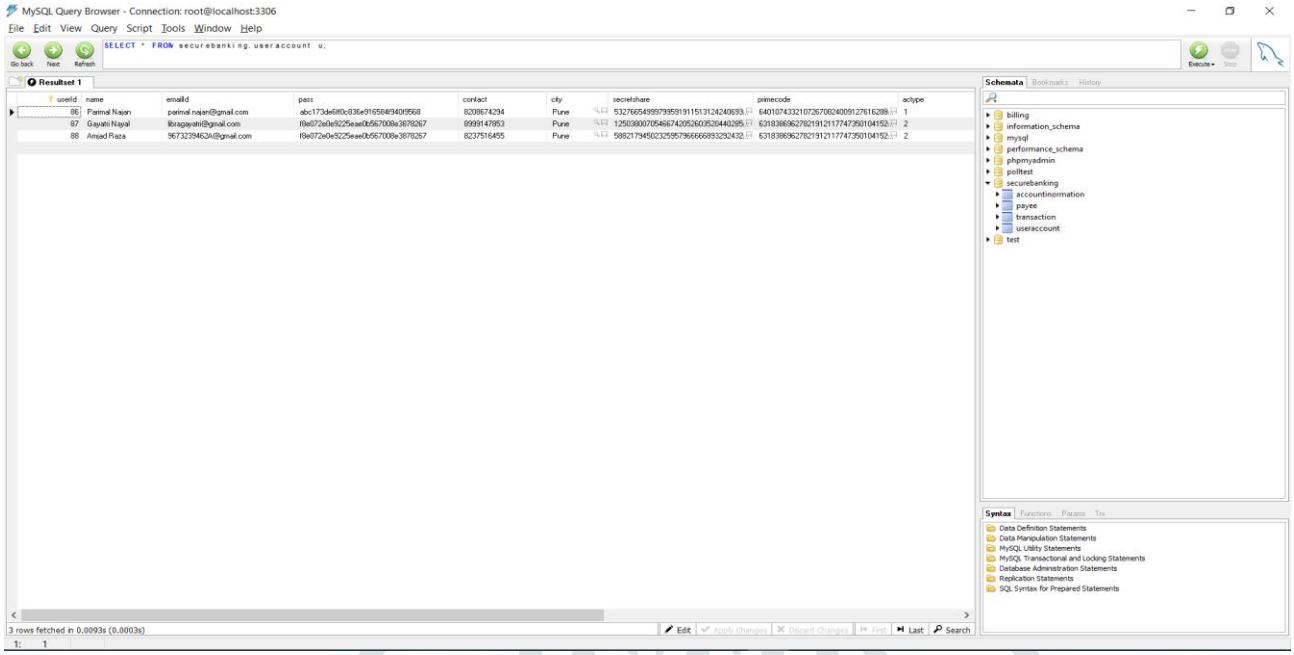

Figure: - Dataset Details

VII. CONCLUSION

The paper gives a brief idea about the implementation of Securing online banking using Visual Cryptography technique. We have also conducted a survey of different methods used by the researcher for visual encryption technology. By reviewing all the paper we come to know that none of the present systems can give 100% accuracy in terms of protecting the data from phishing i.e. intention of obtaining sensitive account related information like your Internet Banking User ID, Password, PIN, credit card/debit by unauthorized users.
We explained a system which can avoid the anonymous data stealing through phishing attack as well provide advanced authentication for joint account holders to access their bank account. The system gives security to banking system and prevention against phishing attacks and Provide trusted authentication.

REFERENCES

[1] SozanAbdulla,"New Visual Cryptography Algorithm For Colored Image",JOURNAL OF COMPUTING, VOLUME 2, ISSUE 4, APRIL 2010, ISSN 2151-9617 HTTPS://SITES.GOOGLE.COM/SITE/JOURNALOFCOMPUTING/.

[2] InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung-Kyu Lee, Member, IEEE"Color Extended Visual Cryptography Using Error Diffusion",IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 1, JANUARY 2011.

[3] DivyaJames,MintuPhilip,"A Novel Anti Phishing framework based on Visual Cryptography",2012 IEEE.

[4] Roberto De Prisco and Alfredo De Santis,"On the Relation of Random Grid and Deterministic Visual Cryptography",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014.

[5] XingxingJia, Daoshun Wang, Member, IEEE, DaxinNie, Chaoyang Zhang, Member, IEEE,"Collaborative Visual Cryptography Schemes",Transactions on Circuits and Systems for Video Technology, 2016.

[6] ShreyaZarkar, Sayalivaidya, ArifaTadvi, TanashreeChavan, Prof. AchalBharambe "Image Based Authentication Using Visual Cryptography and Encryption Algorithm ", International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1692-1696.

[7] Mrs. A . Angel Freeda ,M.Sindhuja , K.Sujitha"ImageCaptcha Based Authentication Using Visual Cryptography", International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2 , April - May , 2013.

[8] DoshiRuchali 1 , Kale Prajakta 2 , PasalkarPranoti "Secured Transaction System Using Steganography and Visual Cryptography",2016 IJESC

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

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

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

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

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

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