IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11448

A Lightweight Authentication system for Digital Banking using QR code

Saurabh Taware[1], Rutvik Naibal[2], Prathamesh Bhujange[3], Rutuja Patil[4],

Prof. Kishori Shimpale[5]

Student, Department of Computer Engineering, SKN Sinhgad institute of technology and science, Pune, India[1,2,3,4]

Assistant Professor, Department of Computer Engineering, SKN Sinhgad institute of technology and science, Pune, India[5]

Abstract : In the area of the internet, various online attacks have been increased and among them the most popular attack is phishing. Phishing is an endeavor by an individual or a group to get personal confidential information like passwords, credit card information, etc from unsuspecting victims for identity theft, financial gain, and other fraudulent activities.

The proposed approach can solve the problem of phishing. An image-based authentication using Visual Cryptography (VC) is used. Visual Cryptography is a secret sharing scheme which owns the technique of sharing visual information. The QR (image) is getting divided into two shares. Here the secret QR is divided into two irregular patterns of images called shares and they can be unraveled without any complicated cryptographic computation.

Keywords: Secure Server Verification, Secret QR, Visual Cryptography (VC),Card Verification Value, RSA Algorithm.

INTRODUCTION

Now days, Online transactions are very common and various online attacks are present behind this. Phishing is one kind of attack in which confidential and sensitive information can be gained by the attackers. Phishing is identified by major attack among all online attacks and new innovative ideas are arising with this. 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. Attackers host a website which is similar to the banking website and attackers bombard emails to some random users. They request the users to update their password for the safety. The mail contains the to the fake website. Attackers use the replica of the original website misguiding the user that it is a banking website or a government website .Users fill in the confidential information and attackers pull the information to their own illegal website. The attacker takes the advantage of it. After collecting this confidential information from the user they login to the actual banking website with the help of the login id and password provided by the user and they transfer the money from the users account to their account. Thus phishing is the indirect way of stealing money online the user. To avoid phishing the proposed system is implemented 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 ”A Lightweight Authentication system for Digital Banking using QR code ” 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 unraveled without any complicated cryptographic computation.

- **Assumptions and Dependencies**

• Assumptions:

– Admin must have basic knowledge of computer.
– User must be used to applications.
– As it is an application user must have smart phones.

• Dependencies:

– Only Administrators will be able to edit main configurations.
– User must have internet connections.
– User must have smart phone to have access from anywhere

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11448

PROPOSED APPROACHES

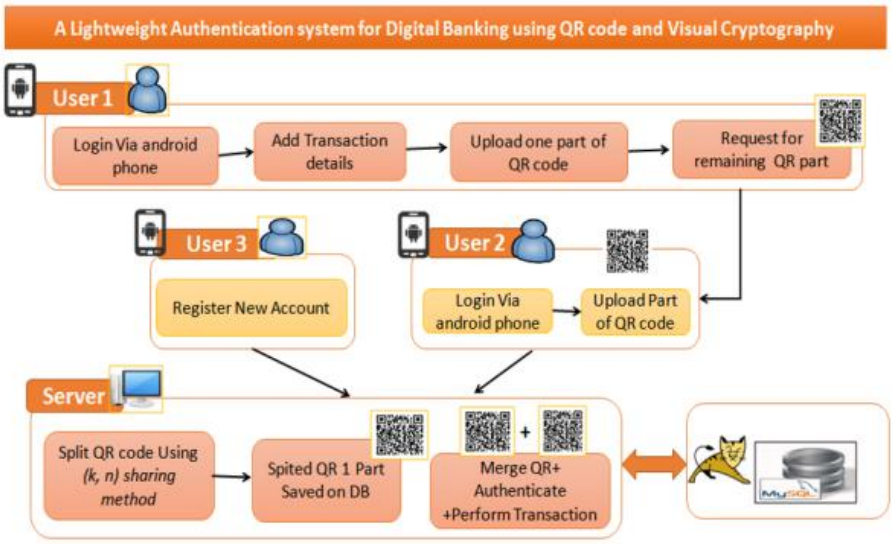


Fig: System Architecture

To avoid phishing the proposed system is implemented with the visual cryptography algorithm and encryption algorithm which helps to increase the security while doing transaction. We have proposed a new approach 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 unraveled without any complicated cryptographic computation. The proposed methodology is implemented using J2EE (Servlets as a Server side technology).

- **Mathematical Model**

Let us consider S be a Systems such that S= {U, Es, Ss, K, DE, Ds}, where
• U= {U1, U2, U3, ...Un | U is a Set of all USERS }
There may be number of users for making use of system. So this is the Infinite Set.
• ES = {E REG, E ENC, E DEC | ES is a Set of Encryption Service }
This service uses the AES and RSA algorithm for Encryption of a file. There are three services provided by this ENCRYPTION SERVER. So this is a Finite Set as this contains limited attributes.

- **RSA Algorithm**
- 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,
1. 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.
2. Compute n = pq.
n is used as the modulus for both the public and private keys
3. Computef(n) = (p − 1)(q − 1) where f is Euler's totient function.
4. Choose an integer e such that 1 < e < f(n) and greatest common divisor of (e, f(n)) = 1; i.e., e and f (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.
5. Determine d as:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11448

D = e − 1mod(?(n))
d is the multiplicative inverse of emodf(n). This is more clearly stated as solve for d given (de) = 1 mod f(n).
d is kept as the private key exponent.
By construction,d ∗ e = 1modf(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 f(n) must also be kept secret because they can be used to calculate d.)

TEST CASES & TEST RESULTS:

The screenshots of test cases is shown in below figure

Test case id	Test case description	Test steps			Test status (P/F)	Test prority
		Step	Expected	actual		
T1	To verify Login name And password.	Enter login name and password	If Username and Password are correct then message "Login successful" and directed towards the next page.	Get the home page	P	High
		Enter invalid login name and password	If username or password are incorrect or any one of them is blank then show error message as "Please enter correct Password".	Display error Message.	P	High

Fig. Test Cases

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

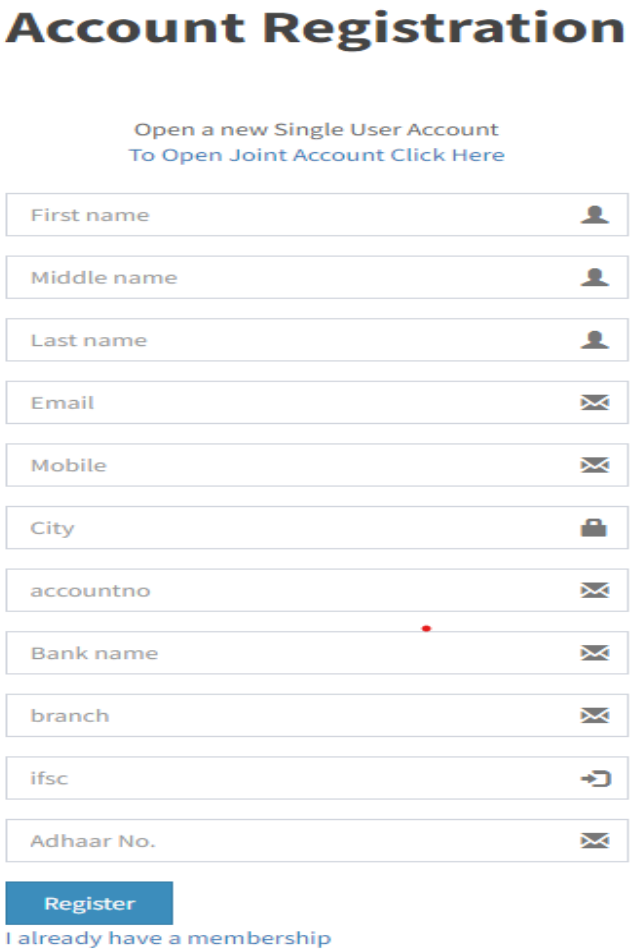
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

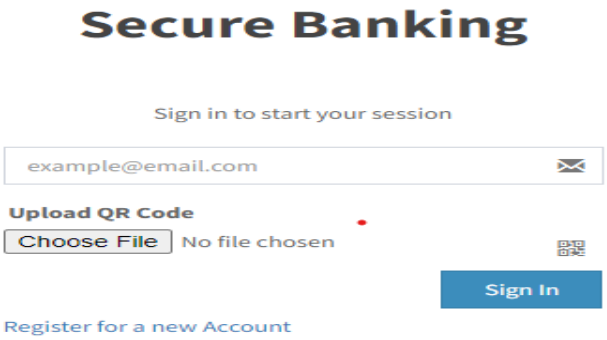
DOI: 10.17148/IJARCCE.2022.11448

Results:

- Registration Page



- Log-in page



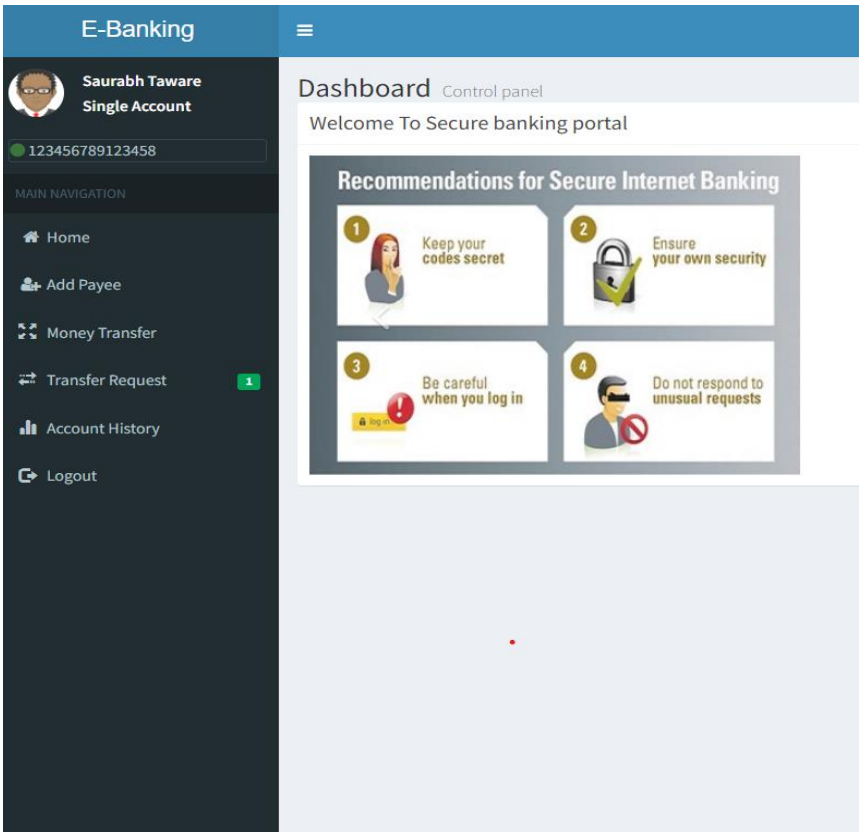
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11448

- Home page



CONCLUSION

Security is a main concern of web users, mainly when using banking applications. Every time user requests a transaction from their bank, the server must be verified to eradicate any chance of fraud. But present systems are not as much secure as the fraudster may create a fake server that asks the user for their banking credentials. There have been many cases of users falling for a fraudster's web application and entering their credentials. The proposed 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. System gives security to banking system and prevention against phishing attacks and Provide trusted authentication.

REFERENCES

1. Shami r, "How To Share a Secret," Commun. ACM, vol. 22, pp. 612–613, 1979.
2. G. R. Blakley, "Safeguarding 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 weenThres hold 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 met hod," 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.