ISSN No:-2456-2165

Authentication in Net-Banking using a QR Code-based safe OTP delivery system

ARNAB SRIVASTAVA - 20SCSE1290002
MAYANK TIWARI - 20SCSE1010986

Abstract:- The customer may quickly and efficiently log into the system under the suggested approach. We examine the suggested scheme's security and usability, as well as its resistance to login credential hacking, shoulder surfing, and unintentional login. The adversary can employ the shoulder surfing attack to steal the user's password by glancing over the user's shoulder while he types it. We've offered secure device schemes with different levels of resistance to shoulder surfing because we've given you secure device schemes with different levels of resistance to shoulder surfing. To use this authentication device, the customer must first register with it by providing basic information. After completing the registration process, the user will be granted access to the login page he or she must first authenticate the account by providing the e-mail address and password that was entered during registration. After the person's email identification and password have been verified, he or she can advance to the next authentication phase, where he or she must choose between a QR (quick response) Code and OTP (one-time-password) (Time Password).After the person's email identification and password have been verified, he or she can advance to the next authentication phase, where he or she must choose between a QR (quick response) Code and OTP (one-time-password) (Time Password). When the customer picks QR Code as the authentication method, the system will produce a QR Code and send it to the customer's email address through the internet. If a person selects OTP, SMS may be delivered to his or her registered mobile number. If the user goes through the login process, the gadget will take them to the main page. At the moment of login, the QR Code and OTP are created at random by the system.

I. INTRODUCTION

Internet banking is one of the most important systems that web users utilize on a daily basis. The number of people using this computer has risen by a significant amount. Even while the majority of banks say that net banking provides 100 percent online security, many customers are hesitant and want more stringent security requirements. Remote authentication of users is an important function in this system to protect against unauthorized access to user records. Lamport was the first to use a 1-way hash chain to implement a one-time password authentication mechanism in 1981. As a result, the number of hash values that may be used to build a collection of passwords is limited. However, in today's world, several authentication procedures are employed at some point in the online banking process. The majority of them entail the use of one-time passwords, and they are limited to the methods of delivering them to users. Time Passwords (OTP) are passwords that are valid just for a session and are used to verify the user within a set amount of time. As a result, the user's use of the new OTP may be validated for each session. They're also useful for preventing replay attacks, phishing attempts, and other types of attacks against primary static passwords. They also give many qualities like anonymity, portability, extensity, and the ability to protect data from being leaked. Textual content messages with the use of a gateway, proprietary tokens, internet-based tactics, comfy Code devices, and Grid papers are a few of the OTP transmission ways. The latest Grid document stores a hash-type file to confirm the user's authentication request, which raises the risk of manipulation. However, they all deal with textual content-based strategies that can be recognized indefinitely. QR codes [6] are used to store textual data in the form of images that can be scanned by any smart device, including most cell phones. QR codes may be thought of as two-dimensional bar codes. There have been a lot of studies done recently that focus on QR code software and the development of the generation for delivering a better human experience. The authors of [7] proposed a contextual QR code recognition approach that might be used to give records relating to certain issues through QR codes. In the field of cryptography, QR codes have been used to safeguard information. Hsiang-Cheh Huang et al. suggested an information hidin2g technique based on QR code software. The authors examined QR codes embedded in images and demonstrated the feasibility of the suggested gadget.QR codes may be used for several things. Algorithms have been suggested and tested that will allow QR codes to be used in electronic ticket machines. AES is a well-known symmetric encryption method. Apart from information security, it's been used in a variety of applications. A method that uses the energy of the AES technique for the creation of an anti-theft system has been cautioned by the authors.

II. RELATED WORK

Clarke et al. were probably among the first to propose using camera-based devices as a more secure authentication mechanism for essential transactions in 2002.

Fig. 1: Comparisons of QR and Barcode

ISSN No:-2456-2165

Denso-Wave, a Toyota eastern agency subsidiary, adopted QR codes (quick response codes) in 1994. Originally designed as a quick means to preserve the sound of vehicle parts, these codes are now extremely popular in Asian nations like Japan, South Korea, China, and Taiwan, and are becoming increasingly popular in western countries by the day. We can use this element to provide QR code use authentication for any structures, including computers, tablets, and mobile phones. We employ element authentication and acquire the notion from the article, which is pertinent to our task.We may also update the call for draught and cheque using coins Card by utilizing this project.

III. PROPOSED AUTHENTICATION SCHEME

The machine is made up of an internet service provider that can create alpha-numerical OTPs using pseudo-random numbers and current timestamps. The usage of timestamps adds to OTP's security and specialization. The alpha-numerical password string was then encrypted with sophisticated Encryption, which is now popular (AES). The ATM pin of the customer is crucial to the set of rules since it is unique to each user and may be obtained using a bank server at each login consultation through the account range. Because the AES set of rules is no longer the best, it is utilized here because it not only provides more safety, but it also improves overall performance in such critical structures. After that, the encrypted string is turned into a QR code through the banking institution's server, you can see a picture. It is then sent to the concerned user through SMTP using e-mail as the communication channel. The user then downloads the QR code image and imports it into the current software made available to him by a net banking provider. The app prompts the customer to submit a QR snapshot, after which he inputs his ATM pin, which is utilized to decode the string study from the QR code. The pin is validated by making an HTTP request to the bank's server. The tool displays the OTP that was produced for that session if the ATM pin is input successfully. The customer next enters the one-time password (OTP) for net banking.This completes the authentication process. Then, on the service company's website, any form of the transaction can be completed.

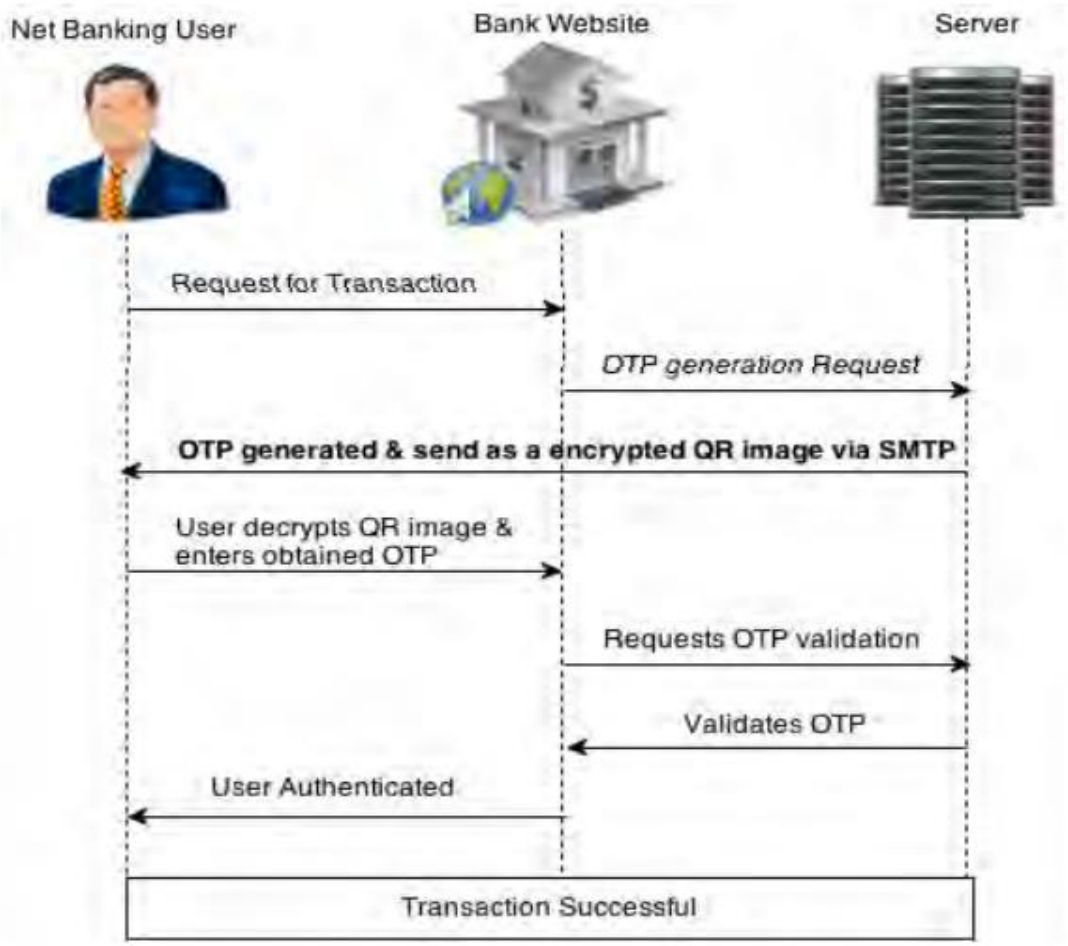

Fig. 2: Sequence diagram for the proposed authentication scheme

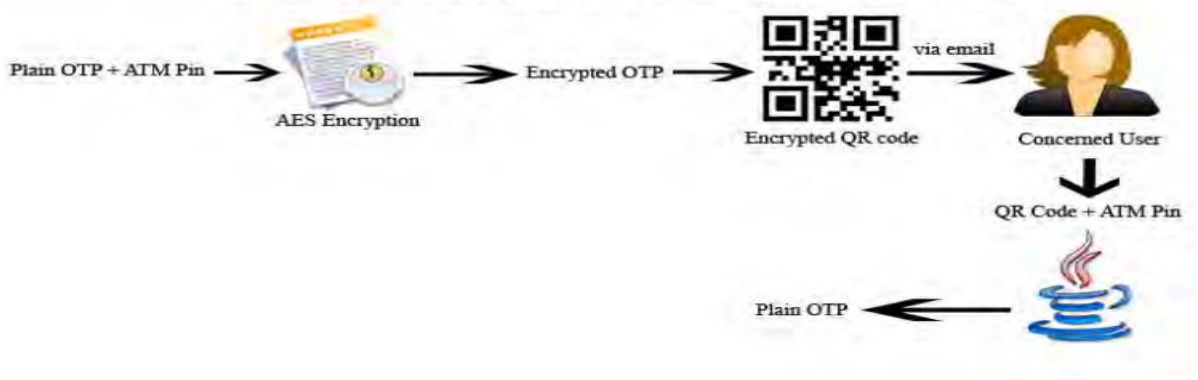

Fig. 3: Workflow of proposed authentication scheme

IV. IMPLEMENTATION

The problem with QR codes is that there is a lack of understanding amongst companies worldwide about individuals who want to expand and use them. QR code-based authentication is advantageous to a person in terms of cost and time. Furthermore, no external tools may be required (along with scanners). Authentication is done using the available id password and OTP, which is never secure. QR code-based authentication device that works on various types of devices, including computers, medicines, smartphones, and so on.

The creation, authentication, and transaction modules are all included in this machine.

A. Creation

The user information and system-generated information are both stored in the creation module. The User must provide his name, address, and a valid cell phone number throughout the sign-up procedure. The user must have a working mobile phone.

The system will produce a unique QR code and OTP for the mobile when the user enters the personnel data. The registration will be successful after reading the QR code and entering the OTP again.

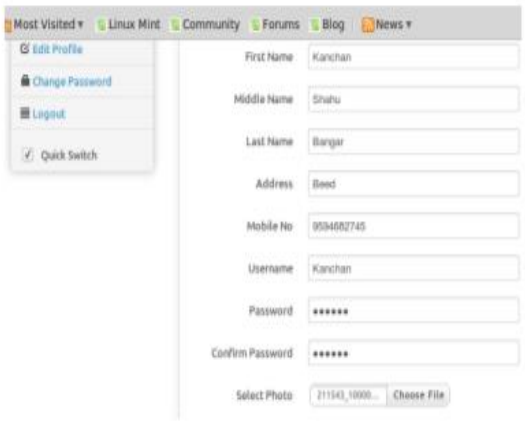

Figure 2: Registration

Fig. 2: Registration

B. Authentication

The system must provide a login screen on the person's hardware device to give the highest level of security as a web application. The user's credentials will be their user ID and password, as well as a scan of a specific QR code. After the user ID, password, and QR code have been verified, an OTP will be delivered to the user's correspondence number, which will be re-entered by the user. Before the user obtains access to the system, the values will be checked by the system.

C. Transaction

A transaction can be completed in one of two ways: by Direct Transfer or through the use of a Cash card.

a) Transfer:
We select the Direct Transfer option in this mode. The user must next specify how many amounts are to be moved, as well as a statement that explains why that particular amount is being transferred. The QR code will then be scanned, and if it matches, the transfer will proceed.

b) With a Cash Card:
We can use the Cash Card instead of a DD or a Cheque. In this mode, we choose who we want to pay, how much we want to pay, and what reason we want to pay.

The system will generate an OTP, which is a unique QR code for Cash Card that QR Code will be thoroughly examined, and if it matches, then only Cash Card will be used to complete the transaction.

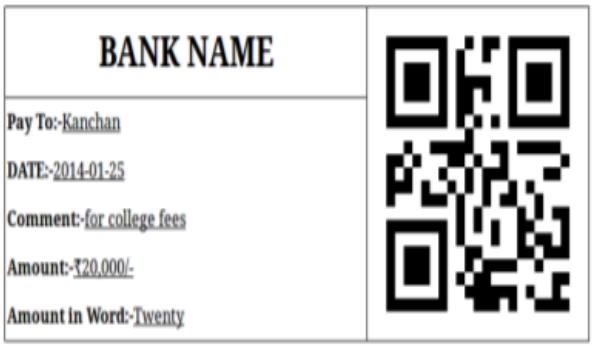

Fig. 3: Cash Card

ISSN No:-2456-2165

V. DISCUSSION

The device's total performance depends on the built-in digicam, which is used to scan QR codes. When we utilize the high-resolution digicam, the device's entire performance improves. Because we do online payments with financial institutions, security is a crucial feature of this device. We also provide OTPs with QR codes; if both are valid, the consumer's authentication and the transaction will be successful. Is it possible to find out how portable the gadget is in this section? Our gadget is hardware agnostic, which means it may be used with any hardware structure, including computers, capsules, and cell phones. It is not always necessary to print the required QR code on the most effective paper; instead, we shall print use the QR code in different places and try different things with it. As a result, it's simple to keep track of. The person's login will consist of a user name, password, and a scan of his unique QR code. OTP may be sent to the consumer's correspondence range after checking the consumer's identification, password, and QR code, and then OTP could be re-entered by the customer. Before the consumer has access to the device, the device will establish the values.

VI. SECURITY ANALYSIS

OTPs are sent in the form of an image, making it difficult for an intruder to determine the location of protected documents. An email message with the OTP is forwarded to the concerned person. Customers using internet banking may quickly gain access to their e-mail accounts and obtain the encrypted OTP by scanning a QR code. As a result, an application software implemented by the bank with the QR photo could most effectively be understood under a secure transmission of the QR code. In addition, the use of the AES set of rules for encrypting one-time passwords adds to the system's security. The proposed scheme is more sophisticated than any existing structure, and it will almost probably take longer to crack the system and might last longer than the useful life of OTPs. OTPs are created for consultation and have a limited lifespan. After the OTP has expired, it is no longer able to use it. The technique is consumer-friendly since QR codes may be recognized. Even a novice user with basic knowledge of how to operate a laptop system may adjust to it.

VII. APPLICATIONS

- Can update smart card: Experimenting with the clever card necessitates the use of a second scanner. According to the QR code, the smart card has a lot less storage.
- Can be used in place of a swipe card: A swiping card can be duplicated, while a QR code cannot. In comparison to QR codes, Swipe Cards have no memory.
- Convenient transaction: QR codes are scanned using a digicam equipped with a hardware device, allowing our technology to provide a more convenient transaction.
- Coins Card: Switching may also be done using a coins Card, which is replicated to demand Draft and Cheque. The device will print a currency card with a QR code for secure authentication.

VIII. FUTURE ENHANCEMENT

The process of converting a picture into more images is known as visible cryptography. By physically shielding these photos over one another, authentic photographs may be obtained. Overlaying an image on top of another may also be accomplished using software programs. The QR code may be converted into two images using visible cryptography, and both of these snapshots can then be sent one after the other. Even if the intruder obtains one of the photographs, he will not be able to decipher the plan without knowledge of the opposite equivalent section of the image. As a result, transparent cryptography may be used to enhance the overall security of the machine. In addition, there is a java utility for decrypting QR codes Image may be readily deployed as cloud software and made available to the intended target market.

IX. CONCLUSION

In this work, we provide a novel authentication method for internet banking that leverages QR code-based OTPs in this paper. The number of individuals who utilize online banking has increased considerably in recent years. As a result, the suggested computer meets the high-security needs of online users and protects users from a variety of security threats. Furthermore, the system has no technical prerequisites, making it very user-friendly. As a result, QR codes have shown to be adaptable and useful in improving efficiency for both users and companies. As a result, it is far more routinely utilized by most firms to market and promote their products.

REFERENCES

[1.] Clarke, Dwaine; Gassed, Blaise; Kotwal, Thomas; Burnside, Matt; van Dijk, Marten: "The Untrusted Computer Problem and Camera-Based Authentication". Lecture Notes in Computer Science, 2002, Volume 2414, Pervasive Computing, Pages 114-124, Jan.2002.

[2.] L.Lamport, "Password authentication with insecure communication, "Communications of ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[3.] Kuan-Chieh Liao, Wei-Hsun Lee, Min-Hsuan Sung, Ting-Ching Lin, "A One-Time Password Scheme with QR-Code Based on Mobile Phone", Fifth International Joint Conference on INC, IMS and IDC, 2009, pp 2069-2071

[4.] Kuan-Chieh Liao, Wei-Hsun Lee, A Novel User Authentication Scheme Based on QR-Code, JOURNAL OF NETWORKS, VOL. 5, NO. 8, AUGUST 2010, pp 937

[5.] Sang-Il Cho, HoonJae Lee, Hyo-Taek Lim, Sang-Gon Lee, "OTP Authentication Protocol Using Stream Cipher with Clock-Counter", October 2009.

[6.] J. S. Tan, "QR code," Synthesis Journal, Section 3, pp. 59-78, 2008.

[7.] Jose Rouillard, "Contextual QR Codes", Proceedings of the Third International Multi-Conference on Computing in the Global Information Technology (ICCCGI2008), Athens, Greece, July 27-Augst 1, 2008.

[8.] Hsiang-Cheh Huang; Feng-Cheng Chang; Wai-Chi Fang, "Reversible data hiding with histogram-based difference expansion for QR code applications," Consumer Electronics, IEEE Transactions on, vol.57, no.2, pp.779,787, May 2011
[9.] Conde-Lagoa, D.; Costa-Montenegro, E.; Gonzalez-Castro, F.J.; Gil-Castiñeira, F., "Secure eTickets based on QR-Codes with user encrypted content," Consumer Electronics (ICCE), 2010 Digest of Technical Papers International Conference on, vol., no., pp.257,258, 9-13 Jan. 2010
[10.] Qiu-Xia Wang; Tie Xu; Pei-zhou Wu, "Application research of the AES encryption algorithm on the engine anti-theft system," Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on, vol., no., pp.25,29, 10-12 July 2011