Two Factor Authentication Using QR-Code

[1]Prof. Shital Patil, [2]Ms. Gayatri R. Burkul, [3]Ms. Anuradha S. Ghuge, [4]Ms. Sujata R. Barke, [5]Ms. Kanchan D. Nehe

Department of IT Engineering
SVIT Nashik, Maharashtra, India

***Abstract*: With the rapid expansion of wireless communication technology, user authentication is becoming increasingly vital in order to assure the technology's security. Passwords serve a vital part in the authentication process. During the authentication procedure, the user's password is sent along with the traffic to the authentication server, allowing the server to grant access to the authorised user. The attackers will take advantage of the opportunity to try to sniff out other people's passwords in order to carry out illicit acts under the guise of someone else's identity, keeping them out of trouble. Many methods have been offered to improve the security of wireless communication technologies as a result of the challenge. In this paper, the previously proposed solution will be used to enhance the security of the system. The solution adopted is the one time password, hashing and two-factor authentication. There also a new solution will be added by using the QR code to help to save more data. The objective of the system outcome is to enhance the current login authentication system. It provides solutions for making password breaking more difficult as well as convinces users to choose and set passwords.**

***Keywords*: Authentication, Factor, Saas, HCMA, HMAC, IOS, U2F, TOTP, OTP.**

INTRODUCTION

Authentication is the process of verifying the identity of the person who desires to undertake the action.
During the authentication procedure, the user's password is sent along with the traffic to the authentication server, allowing the server to grant access to the authorised user.
The attackers will try to sniff the network for data that includes the user's password when the password is transferred.
According to Pagliery (2014), 47 percent of adult accounts in the United States were hacked in 2014.
Hackers have access to their personal information.
As a result of the problem, more people are losing faith in passwords as a means of protecting their online accounts. According to Sulleyman(2017), some of the attackers will earn by selling the compromised email account to others. It is critical to safeguard our own accounts because our credit is valuable. In the cyber realm, it is difficult to track down the attackers. To maintain cyber-security, a secure login system is required. As a result, because the present login system is not safe enough, this project would like to enable other ways to log in to a system.
Many of the services we use on a daily basis, such as banking, have evolved from traditional customer services to Internet-based services. Strong authentication is essential as services containing sensitive data migrate to the Internet in order to ensure a sufficient level of security and privacy. People are increasingly depending on public computers to do business through the Internet, making it a preferred environment for a variety of e-services such as e-commerce, e-banking, and so on. Security is a critical enabler for these applications. In general, a password-based authentication technique provides the bare minimum of security against unwanted access. One-time passwords make gaining illegal access to restricted resources more difficult. Many academics have worked hard to develop OTP methods that use smartcards and time-synchronized tokens or SMS.

MOTIVATION:

The goal of this project is to create a secure login authentication system that uses two-factor authentication.
1) Using the idea of two-factor authentication, the login system's security might be improved.

PROBLEM DEFFINATION:

The current method uses an OTP that is delivered to the user through SMS or email, which has its own set of drawbacks, such as having to wait for an SMS on every login attempt and security concerns.
However, evaluating various attacks renders this system ineffective.
A two-factor authentication system, which uses a password as the first factor and a randomly generated code as the second, is an alternative to this approach.

LITERATURE SURVEY:

E-Authentication system with QR Code & OTP
Authors: Afrin Hussain, DR. MN Nacchappa

Because a quick online configuration is being produced and people are becoming more aware, even budgetary ventures are being involved in the web field.
Hacking is any specialised use of a computer to control the normal operation of system associations and linked frameworks.
The current web banking system was exposed to the risk of hacking and the consequences that resulted, which could not be overlooked.
Individual data has recently been leaked through a high-level approach, such as Phishing or Pharming, which involves obtaining a

client's ID and password.
As a result, a secure client confirmation architecture becomes even more fundamental and important.
Propose a new Online Banking Authentication framework right now.
This verification system combined Mobile OTP with a QR-code, which is a type of 2D standardised recognition.

TS2FA: Trilateration System Two Factor Authentication
Authors: Ali Abdullah s. Alqahtani, Jean Gourd, Hosam Alamlesh, hend Alnuhait

Two-factor authentication (2FA) systems implement by verifying at least two factors. A factor is something a user knows (password, or phrase), something a user possesses (smart card, or smartphone), something a user is (fingerprint, or iris), something a user does (keystroke), or somewhere a user is (location). In the existing 2FA system, a user is required to act in order to implement the second layer of authentication which is not very user-friendly. Smart devices (phones, laptops, tablets, etc.) can receive signals from different radio frequency technologies within range. As these devices move among networks (Wi-Fi access points, cell phone towers, etc.), they receive scattered messages, some of which can be used to collect information. This information can be utilized in a variety of ways, such as begin a connection, sharing information, locating devices, and, most appropriately, identifying users in range. The principal benefit of broadcast messages is that the devices can read and process the embedded information without being connected to the broadcaster. Moreover, the broadcast messages can be received only within range of the wireless access point sending the broadcast, thus immanently limiting access to those devices in close physical proximity and facilitating many applications dependent on that proximity. In the proposed research, a new factor is used - something WhaW iV in Whe XVeU¶V enYiUonmenW with minimal user involvement. Data from these broadcast messages is utilized to implement a 2FA plan by determining whether two devices are coming or not to ensure that they belong to the same user.

2FA: Two Factor Authentication
Authors: Gayatri Burkul, Anuradha Ghuge, Sujata Barke, Kanchan Nehe
The main goal is to set up a secure login authentication system that makes use of two-factor authentication. Using the concept of two-factor authentication, the login system's security might be improved. In order to log in, the attacker must first get beyond the next line of defence. This system will aid in the improvement of the login authentication process. To be able to recognise complex word commands the next goal is to ensure that the login password is not sent over the network. The password is only encrypted, as opposed to the previous technique, but attackers may be able to decode the data and recover the password. To avoid this, the password with the random key will need to be hashed before the sender transmits the message. It is critical to keep the user's password safe. Aside from that, the third goal will be to create an offline one-time password. This will assist you in completing the login procedure if your Wi-Fi connection is limited or your cell signal is weak. It will benefit those who reside in rural areas with poor phone reception. Finally, the fourth goal is to verify that the system is safe from rainbow table attacks. The rainbow table will serve as a dictionary, with hashes and passwords preferred.

PROPOSED SYSTEM:
We create a one-time password on the user side (rather than the server side) in the suggested method using a smartphone application. This means that users can access their one-time password at any moment. As a result, the server will not send a text message every time a user attempts to login. In addition, the generated password changes after a set period of time, making it a one-time password. The user visits a website and logs in or registers.
The user must now open a pin-protected app on their smartphone and utilise the phone's primary camera to scan a one-time QR code that appears.
The application then uses an out-of-band channel to connect with the server and offer verification of device ownership. The user serves as a link between the authorised device and the authentication entity in this scenario. A new user is required to create an account on the website. The user is prompted to enter his or her login credentials, which he or she does. The user's mobile device is then installed with the mobile application. The user's phone is registered with the server after the mobile application is installed. For further mobile authentication, the user must select a pin. The user account's list of devices now includes a mobile unique ID.A QR code will now appear when the user inputs their credentials in the browser. When requested, the QR code is scanned and the PIN for the mobile application is entered. The user has successfully logged in if the QR and PIN are both valid. Figure 2 shows how QR codes can be used for second-level authentication.

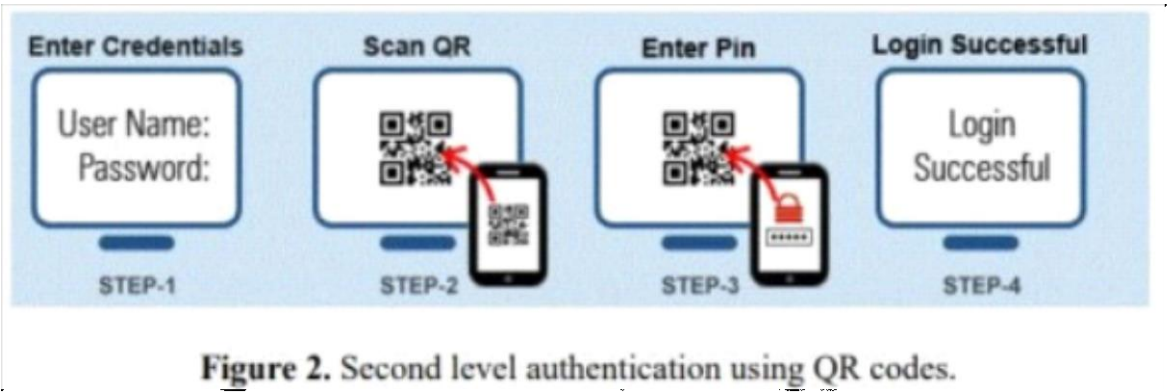

Figure 2. Second level authentication using QR codes.

ADVANTAGES:
1) Helps users to login into their account more securely.
2) Stalker won't be able to collect the password via shoulder surfing.
3) Complex password technique with easy user interface.

LIMITATIONS:
1) Requires a lot of pre-training on audio inputs before achieving peak performance.
2) Word-Error Rate is comparatively low but can be reduced further.
3) Needs a better noise removal algorithm'
4) It takes small dataset to work efficiently.

CONCLUSION:
The OTP can be generated without a connection to the internet, preventing attackers from obtaining the actual password through the network flow. There is a time constraint when implementing the system, which makes it difficult to complete and upgrade the system. One of the most common issues is when the laptop that serves as the system's server is defective. The faulty cause wastes time and money in order to be corrected, and time is squandered throughout the repair process. The system that synchronises the OTP with time in order to create OTP by selecting the random position character of the hashed password can be improved. The login mechanism can also be improved by requiring that the user's password be longer than 8 characters and contain a mix of upper and lower case letters, numbers, and expressions. Now a Days, use of on-line Banking Application are enlarged. Security is a very important issue for handling such services. Therefore the planned system satisfies the high security necessities of the web users and protects them against varied security attacks. This technique is helpful once work once long whereas. On-line banking that involves high security transactions ar created even a lot of extremely protected mistreatment QR codes. OTP distribution is formed accessible by genuine users with the assistance of QR code.

FUTURE WORK:
Two factor authentication is used to implement a secure login authentication system with utilizing with Two-factor authentication. By using the concept of two-factor authentication could help to 4 increase the strength of the login system?

REFERENCES:
[1] 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
[2] Ohbuchi, E., Hanaizumi., H., Hock, L.A, "Barcode Readers using the Camera Device in Cyberworlds, pp.260-265, 2004.
[3] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen ,"HOTP: An HMACBased One-Time Password Algorithm" , , RFC 4226, December 2005.
[4] Understanding Login Authentication n.d. Available from: <http://lia.deis.unibo.it/Courses/TecnologieWeb0708/materiale/laboratorio/guid e/j2ee14tutorial7/Security5.html> (Accessed: 18 November 2017).
[5] Vaithyasubramanian, S., Christy, A. and Saravanan, D. (2015) 'Two Factor Authentications for Secured Login in Support of Effective Information Preservation', 10(5), pp. 2053–2056. Available from: http://www.arpnjournals.com/jeas/research_papers/rp_2015/jeas_0315_1713.p df (Accessed: 18 November 2017).
[6] Kuan-Chieh Liao and Wei-Hsun Lee, "A Novel User Authentication Scheme Based on QR Code",Journal of Networks, VOL. 5, NO. 8, AUGUST 2010
[7] "Two-Factor authentication goes mobile", First Edition September 2012, www.goodeintelligence.com